Design errors in nuclear power plant

Taylor, J.R.

Publication date:
1974

Document Version
Publisher's PDF, also known as Version of record

A. E. K. Risø

Risø - M - 1742

Risø - M - 1742

Title and author(s)

Design Errors in Nuclear Power Plant

by

J.R. Taylor

Date September 1974

Department or group

Electronics Department

Group's own registration number(s)

R-13-74

71 pages + 20 tables + 3 illustrations

Abstract

Abnormal occurrences in nuclear power plant are classified and studied statistically, in order to investigate some aspects of the design error problem.

The objective of the study is to discover what techniques would be useful in reducing the number of design errors in power plant.

Copies to

Abstract to

**Available on request from the Library of the Danish Atomic Energy Commission (Atomenergikommissionens Bibliotek), Risø, Roskilde, Denmark.
Telephone: (03) 35 51 01, ext. 334, telex: 5072.**

Fi 25-204

ISBN 87 550 0289 7

CONTENTS

DESIGN ERRORS IN NUCLEAR POWER PLANT

Introduction

This note started as a study of design errors in process plant, with the objective of finding the most relevant techniques for removing those errors. The most readily available records with sufficient incident detail were the abnormal occurrence reports for light water reactors.

As the study of these reports proceeded, it became clear that the data was very relevant to nuclear power plant reliability analysis, and the objectives of the study were changed. Random component failure due to effects which cannot be prevented, is presumably the most frequent cause of faults in process plant, and is the kind of failure normally treated in reliability analyses. But redundancy techniques and reliability theory seem to have reduced the significance of random component failure in nuclear power plant, until it is only one of several contributors to safety related incidents. Other mechanisms such as operator error, maintenance and installation error, play a large part in these incidents. A significant contributor is design error.

For these reasons, the scope of the study was broadened. All of the abnormal occurrences reported for two power plants during one year were analysed and classified, in order to be able to relate design errors to other causes of failure. To enhance the relevance to reliability analysis, incidents occurring after grant of operating licence were studied, rather than problems during construction. And emphasis was placed on common mode effects.

In what follows, a type study of different kinds of design error is presented, with examples. Then the results of two statistical studies are described, one directed towards classification of design errors, the other towards determining the significance of design errors for reliability. Some conclusions are presented, and techniques for avoiding design errors are discussed.

What are design errors?

A series of cases of design error were studied, and a statistical survey of design errors was made, to enable the effectiveness of design checking techniques to be studied.

In order to make such a study, it is desirable to be able to define what is meant by design error. If one takes the view that all failure is to be avoided, at any cost, then any failure can be regarded as a design error. In practice, this approach is too costly. A designer must accept a certain rate of failure.

A definition of design error which may be acceptable theoretically, is that a design error is considered to have occurred, if the functional specification of a plant component cannot be fulfilled by a given design. But this definition is useless in practice, because functional specifications are rarely made explicit and complete.

A better definition is that a design error is considered to have occurred, if, in the light of experience of use of a system, an alternative design is considered preferable. This definition has a 'disadvantage' that it includes errors which arise because some phenomenon is completely unknown at the time the design was completed. But such 'errors' are also interesting. The definition makes it possible to use a very simple criterion in statistical studies - if the equipment is modified as a result of experience of failure, then the failure was caused by design errors. This criterion will however introduce a bias into statistical studies, because of the effect described in the following quotation

> **2.7** The corrective actions taken in response to equipment failures in many instances have been to repair the equipment or replace it in kind and have not always been guided by a clear identification of the true cause of failure. Analysis of the causes of forced outages in both nuclear related and non-nuclear related equipment suggests that in many instances the design was deficient for the intended service.

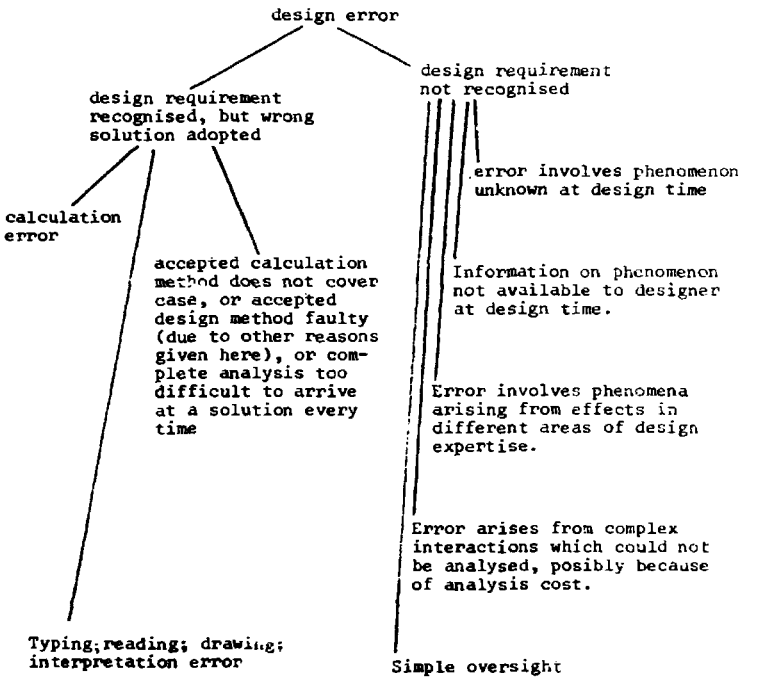


fig. 1 Classification of design errors according to cause.

In the statistical study some attempt was made to correct this bias, by detailed analysis of some frequent types of failure.

Classification of errors is essential, if the effectiveness of techniques for avoiding error is to be judged. A classification of design errors according to cause is shown in fig. 1. It is difficult to apply such a classification to particular cases, because of lack of information. Even interviews with designers cannot always lead to an accurate classification. However, an attempt has been made. The results should be viewed with caution.

The examples which follow are mostly taken from safety related occurrence reports for light water nuclear reactors. The reason for this is not that such reactors are especially failure prone, but because the documentation for nuclear reactor failures achieves a much higher standard and is much more thorough, than for most other types of process plant. This makes study easier. NASA also collect failure data in a similar way, and achieve a high standard of case reporting.

Example 1

In some cases a design error can arise because the necessary information which would allow correct design, is simply unavailable. There is no complete solution to this problem, but materials and prototype testing reduces the problem.

As reported in our letter of September 15, 1971, during an operability test of the High Pressure Coolant Injection (HPCI) system, the HPCI steam line isolation valves tripped closed from a false high steam flow signal. Backflushing of the flow elbow sensing lines appeared to correct the observed increase in the differential pressure measurements from the HPCI steam line elbow taps; however, frequency of testing of the HPCI system was increased to once per week, after its return to service, with additional recording of elbow tap pressures to determine that the observed change in flow elbow differential pressure was not a recurring problem.

On the first weekly test on September 18, 1971, following the return to service of the HPCI system, and while operating at 90% power, it was found that the flow elbow differential pressure had again increased, causing the HPCI steam line to isolate. A review of HPCI tests previous to these two showed that all successful testing had been completed under low main steam flow conditions and that the unsuccessful tests were conducted with approximately 90% of rated steam flow.

Based upon this new information, it was demonstrated that the differential pressure at the HPCI steam line flow elbow, which is directly connected to a saddle on the HPCI steam line, will be affected by the flow in the main steam line. These effects become so pronounced above 50% of rated flow in the main steam lines, that when testing the HPCI system it automatically isolates after 45 seconds because the differential pressure indications remain higher than the reset values of the 150,000 lb per hour flow sensors. This effect on the flow elbow differential pressure prevents full completion of the HPCI system flow rate tests under conditions of high reactor power; however, the conditions under which the HPCI is required to function (low-low reactor water level and high drywell pressure) also result in a reactor scram and a main steam line isolation. Thus,

Docket 50-263

for an automatic HPCI initiation, the main steam flow will drop to zero within 5 seconds and allow the 150,000 lb per hour flow sensors to reset well before the end of the 45 second time delay.

Pending further review of means for development of a practicable method for resolving the flow disturbance effects on the HPCI system steam line elbow taps, quarterly flow rate testing of the HPCI system was planned to be conducted with the "B" steam line isolated for the short period of time required to complete this test. If conditions develop requiring HPCI initiation during the period of testing, proper functioning of the HPCI system will occur as required.

Engineering studies have been completed on various methods to eliminate the flow disturbance effects on the HPCI system steam line elbow taps and the preferred alternate has been determined. We have initiated detailed engineering and procurement of materials to install a Universal Venturi Tube piping section to replace the piece of piping between the existing HPCI steam line flow elbow and HPCI isolation valve MO-2034 as shown on the attached sketch. The new flow device will utilize the existing control logic and where compatible, the existing equipment. The ISA Universal Venturi Tube primary flow metering device will provide sufficient accuracy and reliability, as a replacement for the elbow flow measuring device, to permit flow rate testing of the HPCI system without the need for "B" steam line isolation.

Example 2

When failure effects involve phenomena which cross design specification boundaries, lack of communication between engineers can lead to lack of design analysis and checking. The following incident involving both steam circuits and ion exchange systems, may have been an example of this kind.

The unit was in the process of being started up following a short scheduled maintenance outage when, about one hour after synchronizing the generator, it was noticed that the primary coolant conductivity was increasing. At 1010 hours, the recorder showed 10 µmhos. When grab samples confirmed this high value, a reactor shutdown was initiated at 1020 hours.

An immediate investigation of the cause determined that the resins in the reactor cleanup demineralizer had decomposed due to high temperature. A fresh bed of resins was sluiced into the demineralizer and, following further cleanup of the primary coolant, the unit was returned to service about 28 hours after the shutdown.

Docket 50-155

Febr. 20 1970

The results of the investigation are as follows:

1. The resins had decomposed due to high temperature reactor water being drawn through the demineralizer during blowdown of the primary system for swell during heatup.

2. The operator had not been alerted to the rising conductivity due to failure of the alarm circuit which operates off the recorder. This same failure also prevented the cleanup pump from tripping on high temperature and protecting the resin bed. Inspection of this recorder following the incident revealed that both sets of contacts operated normally with the recorder door open, but would not operate with the door closed. This situation has been corrected.

Corrective actions that have been instituted are as follows:

1. Problems with the alarm and pump trip circuitry have been corrected.

2. The operating procedures have been reviewed and revised to require that the cleanup system be valved out whenever blowdown of the primary system is necessary with primary system pressure above 50 psig. Below 50 psig, the present operating practice will be maintained since, at low pressure, the cleanup pump head is necessary to assure adequate blowdown flow.

In conclusion, no damage to equipment resulted from this incident. The actions of the operating personnel were prompt and proper, and it is felt that the corrective action taken will preclude recurrence.

The only solution to problems of this kind is to improve communication. The information to be transferred involves 'unusual effects' in one piece of equipment and 'unusual consequences' in another piece of equipment. Design review discussions involving several engineers with different specialities can help in this respect. More detailed design specifications including description of possible failure modes could also help in making appropriate information accessible to other engineers, although this in only really possible at the 'Component' level, and not at the system level.

NASA classify errors involving different areas of experience as 'compatability problems'

Accident/Incident Description	Cause	Recommended Preventive/Corrective Action
During verification test of a life support system the test was prematurely terminated due to failure of an oxygen circulation fan/motor within the system to start up, caused by corrosion failure of a fan/motor bearing. Subsequent investigation revealed that the corrosion was caused by water which had been introduced unknowingly into the life support system oxygen loop during a previous spacecraft/life support system compatibility test.	Insufficient compatibility test procedures in that a design limitation of the life support system was not recognized during pre-ordnance development. This limitation allowed water to be introduced unknowingly through a closed water shut-off valve (leakage) in the system, under conditions of test pressure/time span. As a consequence, unreliable oxygen loop dry-out procedures used when water was knowingly introduced into the loop were not implemented.	Require safety review/analysis of safety critical system test procedures during their development, to make certain that the test operations will provide timely removal of all system contaminants that may be introduced by the test conditions.

Manual space program accident/incident summaries 1970-71
Cranston Research inc.
April 1972 N 73-1887

Example 3

In September 1967, approximately 1 year after the incident, following a complete drain of the sodium from the reactor vessel, an object was discovered on the bottom of the inlet plenum. The object was tentatively identified as a segment of zirconium liner from the conical flow guide (see Figs. 2 and 3). Retrieval devices were fabricated and, by the end of March 1968, *the segment was retrieved* and its identity confirmed. The reactor vessel was then refilled with sodium to clean up the oxide deposits that had resulted from the removal operations.

Efforts were then made to remove the remaining segments presumably still attached to the conical flow guide. After fabrication of the necessary tools for the removal operations, the sodium was *again* drained from the reactor in November 1968; it was then that a second segment was discovered missing from the conical flow guide. By the end of 1968 the missing segment had been found lodged against the underside of the lower core-support plate, and all the segments had been removed from the reactor. Figure 9 shows several views of the two detached zirconium segments that were retrieved.

Following *the discovery of the detached zirconium* segments, a series of hydraulic tests was performed which confirmed that the coolant-flow blockage that resulted in the fuel melting was indeed caused by one of the loose zirconium segments from the conical flow guide.

The zirconium liners had been installed in 1959, late in the construction phase, at a time when it was believed that provisions should be made for occurrences which *might result in* substantial fuel melting. The liners were intended to augment the vessel penetration barrier in the lower plenum in the event molten uranium alloy dropped out of the core into the lower plenum.

Six triangular 40-mil-thick zirconium segments were hand-formed to cover the contour of the conical

low guide. Each segment was attached by means of three zirconium machine screws, and the screws were then tack welded to the segments.

The hydrodynamic forces of the coolant had caused sufficient flutter in two of these segments to break them loose from the machine screws by which *they were attached. The hydrodynamic force then* carried one of the segments up to the nozzle inlets and restricted the coolant flow in the general area of the two adjacent subassemblies that subsequently melted.

The abnormal temperatures that had previously been observed in September 1966 and subsequently identified to have occurred in June and again in August *prior to the fuel-melting* incident have since also been attributed to partial flow blockage by one of the loose zirconium segments.[3]

Last-Minute Design Change

The installation of the zirconium liners was apparently made in response to the concern for the consequences of a molten fuel drop as expressed by the Advisory Committee on Reactor Safeguards (ACRS).[4] The response to the concern expressed by the ACRS was *certainly justification for the installation of the* liners, but it is the author's opinion that it did not justify short-circuiting existing quality-assurance procedures. Another point was raised by Representative Craig Hosmer (R., Calif.) in discussing the incident during the hearings before the Joint Committee on Atomic Energy (JCAE) in January and February 1968 (Ref. 4). That point was whether it was easier to install the zirconium sheets – which cost "about a hundred bucks"— than to justify not doing so to the ACRS. The question as considered by PRDC was whether or not to provide the additional "engineered safeguard" prior to buttoning up the primary system and filling with sodium. The decision was in favor of the apparent *increased safety. Upon later analysis it was concluded* that the zirconium segments were not necessary, so all the remaining segments were removed from the reactor in December 1968.

With a little reflection, it should be apparent that when concerns are expressed or decisions are made regarding design, technical problems, or safety issues, they should be attacked with a disciplined engineering approach, with due consideration for codes, standards, *and proof-testing, which make up quality assurance.*

Design changes and repair often give rise to 'simple oversights', for example of a design checking stage.

Example 4

When human beings make a design check, they tend to be led to 'the most likely cause' of failure. This provides a strong argument for cross checking using computer methods, to support the human beings, since the computer can systematically investigate even unlikely causes.

It should be possible to design information systems to help prevent problems like the following series.

1 **Inspection at the time of the first failure of the motor revealed damage had been caused by overheating. After repairs were made, the motor was satisfactorily tested and put into service.** ROE

After the second failure, the motor was again taken out of service and repaired. During post-maintenance inspection of the motor prior to returning it to service, it was discovered that the interpole phasing of the motor was reversed. If the motor had been placed in service, this condition would have led to overheating. 71-8

After the third failure, the motor was again disassembled; this time under the supervision of two qualified technical people. From this inspection, it was determined that the insulation had again overheated, although it met the appropriate specifications. Close scrutiny revealed that the enamel on the rotor windings had not been properly cured. The enamel had softened and the reduction of clearances caused a locked rotor condition which resulted in the overheating of the insulation.

2 **I am writing to inform you of a failure of a motor operated during an operational check prior to Unit ' reactor startup. ·tor was on MO 101, the north emergency condenser condensate valve, :d failed previously this year. This was reported to you in my · dated April 30, 1970.** DOCKET 50-10-71

Unit 1 was shutdown on August 28, 1970, for miscellaneous ; repairs. During a check prior to startup, MO 101 failed to The motor was removed and disassembled and inspection indicated :rheating condition and needed extensive repairs. The motor was .o a local shop for rewinding.

Upon completion of the repairs, the motor was given a final out and it was discovered that the interpole phasing was reversed. ould have resulted in overheating if the motor had been put in ion in this condition. This defect was corrected and the motor turned to service.

3. The Station Review Board reviewed the problem and concluded that the high [illegible] of the torque switch was the cause of the failure of MD-101. As corrective [illegible] the motor was replaced and functionally checked before returning it to [illegible]tion, the torque switches on the valve operator were reset and all packings [illegible] valve were reworked. Additionally, the following program has been implemented to [illegible] the operability of the new motor for the remainder of the operating cycle:

1. Additional insulation has been installed on the valve to reduce operational temperatures.
2. Ventilation has been directed to the motor for additional cooling.
3. A thermocouple has been placed on the motor to monitor operating temperatures, during plant startup.

4. This is to inform you of an occurrence in which a defective motor operator on a Unit #1 Emergency Condenser System Valve was found during investigation into the cause of a 125v DC ground. The failed valve was MD-101, the north emergency condenser condensate valve, which has previously failed three times as reported to you on April 30, September 4 and December 4, 1970.

During the pre-startup checks on the evening of April 13, 1971, the emergency condenser condensate return valves, MD-101 and MD-109, were closed. About one hour after they were closed a 125 V DC ground appeared and was ultimately traced to MD-101.

Inspection of the motor revealed that the insulation had flowed and the windings had low resistance to ground.

The motor was replaced and during testing the motor failed to de-energize when the valve closed. After waiting approximately 20 seconds the operator tripped the breaker manually. The torque switch was reset to a lower value and the valve was operated satisfactorily with the torque-switch de-energizing the motor when the valve closed.

Investigation of the records showed that the torque switch setting had been increased in December, 1969, to reduce leakage through the valve. All failures of the valve have been experienced since that time. It is believed that the high torque setting prevented the motor from tripping as required, thus causing a continuous supply of current to the motor and subsequent overheating of the varnish and insulation on the motor windings.

Example 5

Sometimes interactions in a system are so complex that it is unreasonable to expect a designer to anticipate them, even though the error is classed as a design error.

The cause of the air system failure was the complete rupture of a 6-inch stainless steel flexible connection mounted on the discharge side of Air Compressor 1-2. When the flexible connection failed, it struck the compressor high temperature trip switch which caused the compressor to trip. Air Compressor 1-1 started automatically but was unable to keep up with the air loss.

DOCKET 50 219 - 156

Subsequently, Air Compressor 1-2 discharge valve was closed which isolated it from the air receiver and permitted the air pressure to build up. It is estimated that pressure was restored to normal in approximately 15 minutes. There were no spare flexible connections at the site so a solid spool piece was fabricated and installed to provide a temporary emergency back-up supply of air, and the compressor temperature switch

was repaired. It was also noted that there was axial misalignment of the compressor discharge and the pipe connected to the receiver. This misalignment was corrected prior to installing the temporary spool piece. A rush order was placed for new flexible connections, and the temporary spool piece has been replaced with a new connection for Air Compressor 2-1. The connection will be replaced on Air Compressor 1-1 as soon as it arrives. In addition, a study has been initiated to redesign the compressor discharge piping system to prevent a recurrence of this event.

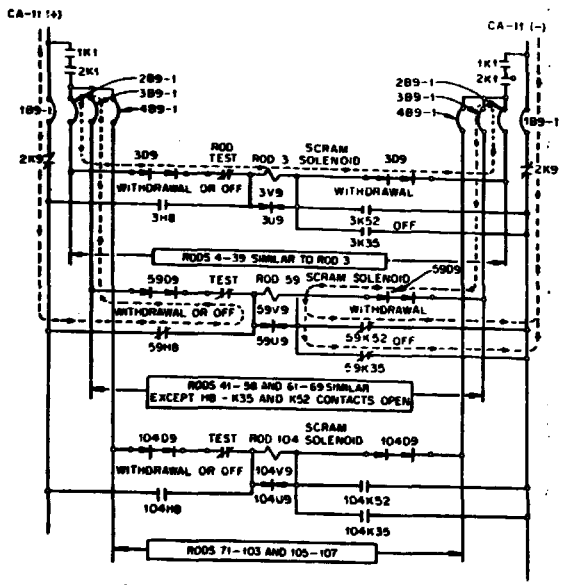
Example 6

In other cases, newer methods, such as sneak path analysis or cause consequence analysis can discover failure potential in such complex systems.

The primary scram system of the N reactor failed to operate on signal because of undetected failures of diodes in the scram circuit. The reactor was shut down promptly, however, by the backup ball safety system. The reliability of the primary scram system was improved, after the fact, by the addition of an administratively controlled switch in the main circuit.

Reactor designers and operators count on the low probability of the failure of any given primary safety system of a nuclear reactor. They do recognize, however, that failures are possible and that effective and independent secondary systems must be available. When a failure occurs, every advantage must be taken of the knowledge gained in the determination of cause and effect. The probable reason for the N reactor diode supply just ahead of the scram relays. When a rod-assignment switch is in the Off or Withdrawal position, this circuit places a holding voltage on the V9 scram solenoid to prevent the rod from scramming if a reactor scram trip occurs. This is a maintenance feature to prevent rods out of service from suddenly moving into the reactor.

Electrical measurements taken across the V9 scram solenoids gave voltage measurements in the range 65 to 95 V, with the highest voltage (95 V) being across 59V9, the rod No. 59 scram solenoid. A current measurement gave about 10 A flowing through the 1B9-1 breaker (breaker trip setting, 12.5 A). Further review indicated that a possible electrical path for connection of the circuits could be developed by the combination of four diodes failing in the shorted mode in the electrical circuit of a rod, along with that rod's assignment switch being in the Withdrawal or Off position. Rod No. 59 became the prime suspect because it was the only rod in the Off position. Figure 2 also shows the current path from the auxiliary circuit through rods 59 and 3. All other rod solenoids would be similarly energized owing to the parallel-wiring characteristics of the circuit. A visual inspection showed that the No. 59 rod diode quad package was cracked and that a drop of solder protruded through the crack midway up the canister. Although the four diodes in a rod circuit are electrically connected as shown, they are physically situated in a plug-in canister called a diode quad package that closely resembles a metallic vacuum tube.



CIRCUIT SHOWN AS FOUND SEPTEMBER 30, 1970
CURRENT PATH SHOWN FOR ROD 3 AND ROD 59
ALL OTHER RODS' CURRENT PATHS SIMILAR TO ROD 3

Fig. 2 Rod-scram solenoid circuit and failure path.

Example 8

Simple oversight is a cause of some design errors, and may have been involved in the following incidents.

Docket 50219

110

The event of the turbine trip was preceded by an oscillation of approximately 2 to 5 MWe in generator load. Steam flow began to fluctuate and reactor pressure decreased slightly. The generator had been operating at 530 MWe, approximately 1600 MWt, and load was reduced to 400 MWe by recirculation flow, when the oscillation ceased. At this point, the turbine tripped.

Upon occasion, the turbine control valve cams have been known to contribute toward an oscillation in load at high valve opening positions due to the control valve loop gain being higher at these positions.

Up to the valve position associated with approximately 500 MWe, the loop gain is constant. However, oscillations can occur above 500 MWe if a perturbation, such as a load swing or pressure spike, were to occur at the higher valve open positions. The perturbation which precipitated this event was the result of load swings brought about while backwashing the main condensers. The remedy has been to reduce the load to a more stable cam position, eliminate the oscillations, and recover to the desired electrical load. In addition, until the cams are replaced, operations which may cause an upset are performed at a lower load.

Example 9

Some simple oversight errors occur several times.

1 ping valves with steam. If this can't be done, test by try-levers. Inspect discharge pipes to make sure it's secure, won't blow away when valve pops. Operators have been killed as valve discharge pipe has ripped like paper with steam at low pressure. Drain-opening in discharge line must not be plugged.

Plant operators

Manual 1965

SM Elonka

2 It was concluded that the probable cause of failure was the actuation of the safety relief valve that was set at 1085 psig. The dynamic loading resulting from the actuation of this valve, combined with the condensate in the line, exerted a bending moment and torsional stress on the header at the location of the valve attachment. Since the architect-engineer had not taken these overstressing forces into account in the original design, the valve attachment was not fabricated to withstand this dynamic loading and the valve tore loose from the header at a point opposite the valve discharge stack. The two other valves failed

ROE

72-15

3. The decay-heat-removal valve that caused the incident is a 4-in. pneumatic valve exhausting vertically through a 4-in. nozzle, which was inserted into, but not attached to, an 8-in. vent pipe that goes through the roof of the building. During the accident the 4-in. line backed out of the 8-in. vent and released live steam into the building, despite the fact that the system had been operated successfully about 20 times previously. It was determined that the equipment malfunction and the personnel injuries were the result of inadequate design of the piping for the secondary steam system.[8]

4. The control system of the decay-heat release valve is designed so that, if a remote manual signal is imposed on the electropneumatic converter, the positioner output pressure will continue to increase until the unbalanced control signal is satisfied by feedback from actual valve movement. If the valve does not open to provide this feedback signal, the positioner pneumatic output pressure will continue to increase until it reaches the pressure that exists at the full-open position of the valve. After the incident the valve was disassembled and inspected, but there were no indications of stem wear.

The release line from the valve normally extended into the sleeve about 4½ in. when no steam was being released. The steady-state thrust resulting from the discharge of steam at the maximum design conditions (330,000 lb/hr at 1085 psig and 556°F) is approximately 7780 lb. This design force would result in a depression of the pipe support hanger to the limit of its travel and in a deflection of 3⅞ in. in the piping at the discharge end of the decay-heat release line but would not cause disengagement from the vent pipe. For this to happen, a force of 8900 lb would be needed. A thrust loading exceeding 8900 lb may have been imposed on the pipe as a result of a dynamic load resulting from rapid opening of the valve to its full-open position.

Example 10

A calculation error.

During the recent refueling outage, it was discovered that the rivet sizing calculations for the main steam blowout panels were based on blowout at 0.5 psid instead of 0.25 psid as described in the Monticello FSAR.

Based on a reanalysis, every other rivet was removed from the juncture of the wall frame and panel frame of each panel. As the panel design is based on rivet shear, utilization of half the number of rivets provides for a design blowout at 0.25 psid.

Docket 50-263
May 23 1973

Statistical study I

Some idea of the significant rôle played by design error can be obtained by studying summary data. In the following two tables, the causes of system failure are presented for the NASA manned space program in 1970-71 and for boiling water reactors in 1970.

For conventional plant design errors are costly, but not much more so than equipment failures due to wear. The proportion of failure attributable to design errors and to equipment failure are similar. Some cases of design error are included in equipment error statistics, due to inaccuracies in reporting. All of this means that failure cost estimates based on equipment failures alone will not be too inaccurate (within an order of magnitude).

For nuclear plant, aircraft, certain military equipment etc. there are some failure modes which lead to expecially severe consequences. Their frequency is fortunately, generally low. It is important, however, to find out if these serious failures are associated with design errors because 'reliability' approaches to design, such as providing safety margins and redundancy, are not so effective in preventing design error failures. For the same reason it is important to know if common mode failures are associated with design errors.

The records of failure reported in 'safety related occurrences reported in 1970' (Scott & Gallaher 1971), for boiling water reactors, were analysed according to cause and seriousness. The cause classifications were

Equipment	E
Design	D
Installation	I
Fabrication	F
Operator/administration	O
Maintenance	M

In making these classifications, heavy reliance was placed on the keywording provided by ORNL staff in their report. In addition, original documents were inspected, and any incident which resulted in a design change, was deemed to result from a design error (This provides a simple criterion).

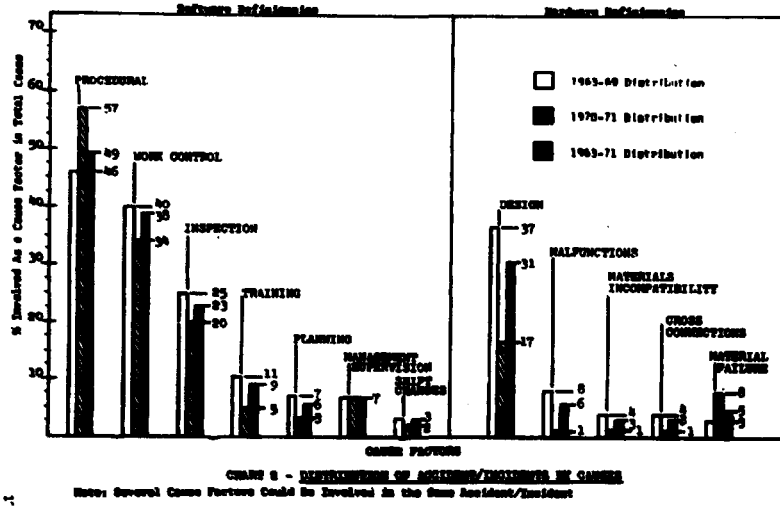


CHART 8 - DISTRIBUTIONS OF ACCIDENTS/INCIDENTS BY CAUSES

Note: Several Cause Factors Could Be Involved in the Same Accident/Incident

Fig. 2

Taken from, Manual space programs Accident/Incident Summaries 1970-1971. (Cranston Research INC. Alexandria Va.) April 1972, N73-1887

Table 1. Summary of BWR Problems

Components			Systems			Causes		
Equipment	%	No.		%	No.		%	No.
Valves	25	(30)	Main cooling	15	(31)	Maintenance error	32	(47)
Pipe	17	(20)	Containment isolation	10	(21)	Operator error	18	(26)
Main steam isolation valves	10	(11)	Safety	10	(20)	Design error	15	(22)
Diesel generator	8	(10)	Control	9	(19)	Installation error	10	(15)
Fuel	8	(9)	Emergency power	8	(16)	Fabrication error	9	(13)
Valve motors	7	(8)	Emergency cooling	5	(11)	Stress corrosion	6	(9)
Gas turbine generator	5	(6)	LPCI	4	(9)	Administrative control	4	(6)
Pump	5	(6)	NPCI	4	(9)	Debris	2	(3)
Control rod drive	5	(6)	Core spray	4	(8)	Vibration	1	(2)
Pipe welds	2	(2)	Core components	4	(9)	Corrosion	<1	(1)
Torus	2	(2)	Containment	3	(6)	Thermal stress	<1	(1)
Jet pump	<1	(1)	Waste treatment	3	(7)	Thunderstorm	<1	(1)
Motor	<1	(1)	Standby gas treatment	3	(6)	Fatigue	<1	(1)
Studs	<1	(1)	Coolant cleanup	2	(5)			
Filters	<1	(1)	Pressure control	2	(5)			
Main steam flow restrictor	<1	(1)	Instrument air	2	(5)			
Turbine blades	<1	(1)	Off gas	1	(2)			
Instrumentation			Stack monitor	1	(2)			
Switch	51	(27)	Turbine	1	(3)			
Relay	20	(10)	Normal power	1	(2)			
Circuitry	13	(7)	Emergency service water	<1	(1)			
Breaker	3.5	(2)	Auxiliary cooling	<1	(1)			
Fuse	3.5	(2)	Pressure relief	<1	(1)			
Amplifier	3.5	(2)	Containment suppression chamber	<1	(1)			
Transformer	3.5	(2)	Containment spray	<1	(1)			
Recorder	2	(1)	Pressure vessel	<1	(1)			
			Building vacuum relief	<1	(1)			
			Feedwater control	<1	(1)			
			Instrument power	<1	(1)			
			Stack	<1	(1)			
			Poison injection	<1	(1)			
			Fire protection	<1	(1)			
			Failed fuel detection	<1	(1)			

Taken from: Safety Related occurrences in nuclear facilities in 1971
R.L. Scott and R.B. Gallaher ORNL-NSIC-106

Table 2. Summary of PWR Problems

Components			Systems			Causes		
Equipment	%.	No.		%.	No.		%.	No.
Valves	15	(11)	Main cooling system	29	(26)	Design error	25	(15)
Heat exchanger tubes	10	(7)	Core components	11	(10)	Operator error	22	(13)
Control rod drives	8	(6)	Safety system	10	(9)	Maintenance error	14	(8)
Radioactivity release	8	(6)	Control system	9	(8)	Fabrication error	8	(5)
Fuel	7	(5)	Safety injection	8	(7)	Installation error	7	(4)
Screens	7	(5)	Radwaste	7	(6)	Vibration	7	(4)
Pipe	6	(4)	Containment	6	(5)	Lightning	7	(4)
Pipe welds	4	(3)	Emergency power	4	(4)	Thermal cycling	3	(2)
Steam generator	4	(3)	Normal power	3	(3)	Debris	3	(2)
Personnel exposure	3	(2)	Turbine	3	(3)	Administrative control error	2	(1)
Pump	3	(2)	Containment isolation	2	(2)	Corrosion	2	(1)
Waste evaporator	3	(2)	Auxiliary building	2	(2)			
Diesel generator	3	(2)	Emergency cooling	1	(1)			
Fire	3	(2)	Pressure relief	1	(1)			
Containment concrete	3	(2)	Pressure vessel	1	(1)			
MSIV	1.5	(1)	Instrument air	1	(1)			
Safety valve	1.5	(1)	Auxiliary cooling	1	(1)			
Containment tendons	1.5	(1)	Coolant purification	1	(1)			
Seal leak	1.5	(1)						
Studs	1.5	(1)						
Thermal shield	1.5	(1)						
Turbine bearings	1.5	(1)						
Turbine blades	1.5	(1)						
Instrumentation								
Circuitry	27.5	(5)						
Relay	22	(4)						
Instrument	17	(3)						
Breaker	17	(3)						
Capacitor	5.5	(1)						
Switch	5.5	(1)						
Transformer	5.5	(1)						

Taken from: Safety related occurrences in nuclear facilities in 1971
R.L. Scott and R.B. Gallaher ORNL-NSIC-106

Some attempt was made to classify the causes of design error, although in no case was there a sufficient evidence for an accurate classification. The entries are largely guesses. The classification used was:

Unknown phenomena/unknown at design time)	V
Complex system effects	C
Cross specialisation, or inter disciplinary problems	S
Oversight	O
Communication problem	K
Calculation or sizing error	Z

A single error could well have many causes.

Table 3

'Seriousness' proved difficult to judge for many of the incidents. A simple Yes-No classification was used, an incident being deemed serious if it involved an explosion; loss of life; unscheduled release of radioactivity; excessive pressurevessel pressure, temperature or temperature rate of change; break of a primary cooling system pipe, or lack of primary cooling system isolation; or disabling of one complete safety mechanism (eg. all shut down rods).

The stage at which the incident was observed was also recorded. because this also has a bearing on seriousness. Many seriou. design errors are detected during commissioning, and do not appear ... operating statistics. It is desirable to gain some impression of how many design errors are found at this stage, since the commissioning tests themselves are not perfect. The stage of discovery classification is as follows:

Early commissioning, before fuel load	EC
Late commissioning, after fuel load	LC
Operation	OP
Maintenance and scheduled testing	MN
Post maintenance test	PM

Table 4

Whether an incident involved common mode failures was determined by an unusual rule - if the failure mechanism affected several components which were previously thought independent, then a common mode failure was deemed to have occurred, even though only one component contributed directly to the failure. This is in accordance with a philosophy of recording 'near misses', as well as 'hits'.

> (2) In general, we take account of that experience which is closest to us and often only that which is dramatic. Too much credit is taken for 300 reactor years of safe operation - meaning only freedom from large accidental releases of fission products, failing to see or adequately to have regard to all those minor and sometimes major features of equipment or of organisation which might so nearly have led to disaster.
>
> 'Farmer, F.R. IAEA-SM-169/43

Provided the rules are applied uniformly, and their definition remembered when interpreting results, no undue bias should be introduced by recording 'near misses'.

Whether a long chain of events were involved in the incident was recorded. Typical long chains of events are a failure leading to level control problems, leading to overflow, leading to turbine or piping damage. Whether the there were several initial independent causes for the incident recorded. Such incidents usually involve 'unrevealed faults' or 'latent' faults.

In order to enable some feeling for the kind of problems involved to be built up, the equipment involved and the failure mechanism involved were recorded using an adhoc classification system.

Table 5

EQUIPMENT CODING

Capacitor	CAP
Condenser	CON
Control	CTR
Control rod	CR
Core	COR
Fuel	F
Gas treatment system	GAS
Heat exchanger	HEX
Insulation (thermal)	THS
Ion exchanger	IEX
Instrument	INS
Level sensor	LVL
Noggle	NZ
Pipe	P
Pipe support	SUP
Potentiometer	POT
Power generator	GEN
Power supply	PWR
Pump	PMP
Pump seal	PS
Recorder	RE
Relay	RLY
Solenoid valve	SOLV
Switch (electrical)	SW
Tank	TNK
Transformer	TFMR
Tubing	TUB
Turbine	TRB
Valve	V
Valve actrator	VACT
Weld	WLD

Table 6 Failure mechanics code

ADJ	Mechanical adjustment
BLK	Blockage
BRK	Broken component
CIR	Short/open circuit
CHEM	Chemical
CAL	Calibration
CLOSS	Loss of control
COR	Corrosion
COUPL	Powerline coupling
CRC	Crack
E	Loss of electric power
EA	Energy accumulation
ER	Energy release
EXPL	Explosion
FL	Unwanted flow
FTG	Fatigue
GOD	Act of god
HYD	Hydraulic effect, water hammer
INF	Interruption of information flow e.g. measurement information
IMP	Steam impingement
IND	Abnormal indication
LK	Leak
LWL	Low water level
LMT	Temperature/pressure excess
LOOS	Loose part
MF	Missing flow
MIS	Impact, missile
MISS	Missing component
NOISE	Instrument noise
RAD	Exposure to radiation
SEQ	Operation sequence error
SNK	Sneak path
STK	Sticking
STR	Stress
SPUR	Spurious information
TH	Thermal (stress)
TRANS	Control transient
VAC	Loss of vaccuum (in condenser etc.)
VIB	Vibration
W	Wear, lifetime exceeded etc.

Table 7. Failure related occurences reported in 1971 for BWR's

ORNL Accession No.	Reactor Age	Cause type	Stage	Serious/not	Multiple cause	Common mode	Accident Mechanics	Design error cause	Reactor	Component		Chain of events
47822		O	MT	Y	N	Y	TIM		Dresden 2	V		
47511		F	M	N					"	F		
47511		E	MT	N	N	Y	TIM,BLK		"	CR		
00077		M	MT	Y	N	N	BCK		"	PMP		
03085										V	?	
56054		D	MT	Y	N	N	TIM	Z	"	HYD ACT	50237-40	
15130		D	MT	Y	N	Y	MF	Z	"	V	50-237-73	
56322		E	MT	N	N	Y	TIM		"	CR		
57235		M	MT	N	N	N	JAM		"	V		
57235			MT	N	N	N	W	U,C		MCH ACT		
57236		I	OP	Y	Y	Y	CIR		"	PWR		
57053		I	OP	Y	N	N	LK			TUB		
61876		I	MT	Y	N	Y	JAM		"	V		Y
58012							TIM			CR	?, there are several of these	
59931		E	OP	Y	N	N	BCK		"	DSL PWR		
60228		O	OP	N	N	N	LMT		"	V		
60228		M	OP	N	N	N	CAL		"	INS		
60227		E	OP	Y	N	Y	BLK			PN ACT		
59924		O									citing	
59928		M	MT	N	N	N	JAM			CR		
59930		D	MT	N	N	N	JAM	C		PN ACT	Design cha. Details 50-237-118	
60226		O	OP	N	N	N	MA,RAD			TNK		
58509		M	OP	N	N	N	MA,RAD		Pasific gas Elec. (Humboldt)	PS		
47509											Qualificat. report	
57228		F	OP	Y	Y	N	CRS		PGE	P		Y
57288		M	OP	Y	Y	N	ADJ		"	MRT ACT		
58016		E	OP	N	N	N	GOD		PGE	PWR		
58506		E	OP	N	N	N	GOD		PGE	PWR		
41462		M	OP	Y	N	N	W		Dairyland Lacrosse	GEN RLY		
41937		D	OP	Y	N	N	BLK	O	"	GEN	Freezing	

ORNL Accession No.	Reactor age	Cause type	State	Serious	Multiple cause	Common mode	Mechanics	Design error cause		Component	Chain of events	
61041		E	OP	N	N	N	OSC,NOISE TRP		Lacrosse	P		
		E	OP	Y	N	N	LK			TUB		
61323		E	OP	Y	N	N	BLK		"	HYP CR		
		D	OP	Y	N	N	JAM	U	"	CR		1155-102
58005		D	MW	Y	N	N		U,Z	Millstone PT.1	GEN		
57474		O	EC	Y	Y	N	W	Z	"	V		
858011		E										
857474		D										
60817		D	MN	Y	N	N	BAL,ADJ	O,Z	"	GEN		50-245-44
60225		D	EC	Y	N	N		Z	"	CON		50-245-47
59927		D	EC	Y	N	N	STR	O		P		50-445-248
		F	EC	N	N	N	MISS		"	V		
		F	EC	N	N	N	W		"	V		
48469		D	EC	Y	Y	Y	STR		Monticello	RL4		50263
56056		E, D	EC	Y	Y	Y	CIR,JAM		"	GAS		50-263-44
57238		MN	EC	N	N	N	ADJ,BLK		"	V		
42742+ others		D	MN	Y	N	N	COR,CRC		Nine mile point	NZ		-?-look at docket 50-220
42743		O	OP	Y	N	N	MR		"	TNK		
60380												Trans Amer Nuc Soc sept. 3 1970
60230		D	LC	Y	Y	N	OSC	C,U		COR		
61325		O	OP	N	N	N	TRIP,LMT		TRIP,LMT			5 cases
43338		E	OP	N	N	N	BLK		Oyster creek			
48957		D	MN	Y	N	Y	JAM	Z		SUP V		? docket 50219
4 23		E	OP	Y	N	N	CRC TAS			GEN		
		D	OP	N	N	N	VIB,LK	O		HEX		
		D	OP	Y	N	N		Z		PMP		
		D	OP	N	N	N	SEQ,TIM	Z		V		
47285		E	OP	Y	N	N	LK,BLK			SL,CR		50-219
48576		E	OP	N	N	N	VAC,TRIP			TRB		
		E	OP	N	N	N	TRIP,LMT			INS		
		E	OP	N	N	N	TRIP LMT			INS		
		E	OP	N	N	N	MOISTRIP			TRB		
		E	OP	N	N	N	CIR TRIP					
		M	OP	N	N	N	LWL,OSC,TRIP			PMP		
		E	OP	N	N	N	GOD TRIP			INS		
15227		O	OP	N	N	N						
58513		D	OP	Y	Y	Y	TIMJAM BRK	O		CR		50-219-105

ORNL Ref. No.	Reactor age	Cause type	Stage	Serious/not	Degree of danger	Multiple cause	Common mode	Accident mechanics	Design error cause	Reactor	Danger due to Domino effect	Component	Comments
42889	6	E	OP	N		N	N	COR		Big Rock Point	N	F	
42000	6	D	OP	N		N	N	CHEM	C		Y	Iex	50-155-24
42000	6	D	OP	N		N	N	CIR	O	"	N	RE	50-155-25
42001	6	D	OP	N		N	N	EXP	C	"		IN	
58510	6	E	OP	N		N	N	COR		"		F	
58510	6	E	OP	N		N	N	COR		"		F	several of these reports
57230	6	E	OP	Y		N	N	CIR		"		PWR	
56320	6	O	OP	N		N	N	MR		"		V	
56320	6	E	OP	N		N	N	CIR		"	Y	PN ACT	
61318	6	E	OP	N		N	N	W		"		PS	
61318	6	E	OP	Y		N	N	CHEM		"		IEX	
61318	6	F	OP	N		N	N	-		"		WLD	
40521		F	OP	N		N	N	CRC		Dresden 1		P	
41527		E	OP	N		N	N	LK		CON ED		CON	4 examples
41527										" "		CR	clearinghouse 22151
45168		D	OP	Y		N	N	LOOS VIB CIR		" "		GEN	50-10
45168		O	OP	Y		N	N	JAM		" "		GEN	
45168		E	OP	N		N	N	CIR?		" "		V	
41568		E	OP	N		N	N	CIR				SW	
45168		E	OP	N		N	N	LK				P	
44751		D	MN	Y		N	Y	BLK	O	Dresden 1		LVL	50-10
44752		I	OP	N		N	N	CIR		"		MTR ACT	
49 0												HYD ACT	
58013		E	MN	Y		N	N	LK				MTR ACT	
60234		F	EC	N		N	N	CIR		"		P	
59932		?	OP	N		N	N	CRC		"		PWR	
41938		M	MN	N		Y	N	CIR		Dresden 2		TFMR	
62110		M	MT	N		N	N	CIR		"		V	
45176		O	MT	Y		N	N	MF,BLK		"		CR	50237-49
44756		?	MT	Y		N	N	TIM Z		"		PN ACT	
47289		E	MT	Y		N	N	JAM		"		MECH ACT	
47290		?	MT	Y		N	N					V,P	
00065		O	OP	Y		Y	N	HYD,CRC		"		PM ACT	
26		I	MT	N		N	N	ADJ		"		CR	
47291								TIM		"		V	50-237-59
47815		D	OP	Y		N	Y	IMP C					
47820		O	M	Y		N	Y	MF					

ORNL Accession No.	Reactor age	Cause type	Stage	Serious/not	Multiple cause	Common mode	Accident mechanics	Design error cause	Reactor	Component		Chain of events
61445		E	OP	N	N	N	FL		Lacrosse	V		
60093		E	MN	N	N	Y	STR COR		"	NZ	may be design - or fabrication failure was inevitable-sensitisat.	
48584		O	MN	N	N	N	STR		"	F		
48019		D	OP	N	N	N	ADJ,IND	C	"	LVL	1155-27	
46958		F	MN	Y	N	N	CRC S		"	NZ		
48020		D	MN	N	N	Y	STR JAM	U	"	F	11533	
58165		F	OP	N	N	N	NOISE	N		INS	4 cases	
		E	OP	N	N	N	JAM					
		E	MN	N							1155-78	
58166		E	OP	N	N	N	NOISE,TRP		"	INS	3 cases	
		O	OP	N	N	N	TRIP		"	PMP		
		O	OP	N	N	N	TRIP		"	INS		
		E	OP	N	N	N	TRIP,W		"	INS		
		O	OP	N	N	N	TRIP		"	SW		
46959		D	MN	Y	Y	N	LOOS,ADJ		"	HYD ACT		Y
27489		E	OP	N	N	N	W TRIP			SW		
		E	OP	N	N	N	NOISE TRIP			INS		
		O	OP	N	N	N			"			
		E	OP	N	N	N	LK		"	PS		
		E	OP	N	N	N	CIR,LK		"	INS		
57471		D	OP	N	N	Y	TRANS,ADJ TRIP		"	PS	115-5	
		E	OP	N	N	N	NOISE TRIP		"	INS		
		O	OP	N	N	N	TRIP			V		
31945		E	OP	N	N	N	NOISE TRIP			INS	several	
		E	OP	N	Y	N	W,LK TRIP,OSC			V INS		
48585		E	OP	N	N	N	W,TRIP		"	CAP		
		M	MN	N	N	N	OSC,TRIP			PMP		
59066		E	OP	N	N	N	CIR		"	PWR		
		E	OP	N	N	N	NOISE TRIP			INS		
		M,D	OP	Y	N	N	BLK	O	"	CR		
32202		MN	OP	N	N	N	CIR			PWR		
		OO	OP	N	N	N	SEQ		"	V		
58173		D	OP	N	N	N	CA		"	INS	1155-83	

ORNL Accession No.	Reactor age	Cause type	State	Serious	Multiple cause	Common mode	Mechanics	Design error cause	Reactor	Componend	Chain of events
56979		D	OP	Y	N	N	OSC	C	Oyster creek	CTL	
		D	OP	N	N	N	NOISE TRIP	O		POT	
		M	OP	N	N	N	BLK TRIP			SC	
56980		D	OP	N	N	N	MISS	O		V	
61706		D	OP	N	N	N	OSC TRIP	U		CTL	
56982		I	EC	N	N	N	FIRE		QUAD Cities	COR	
59925		?	OP	Y	N	N	VIB,MIS		ROBINSON2	GEN	
44649		D	OP	Y	N	N	FIRE	S		TINS	
44918		E	LC	N	N	N	OSC BLK			CTL INS	
00213		D	MN	Y	N	Y	JAM			SOL V	
60860		D	OP	Y	N	N	HYD	O		P	

The contents of this table were abstracted from 'Safety Related Occurrences reported in 1971', R.L. Scott and R.B. Gallagher, 1972, ORNL-NSIC-106.

Many of the classifications were checked against original Docket reports, and the classifications given are the responsibility of this author.

Sources of Bias

While the statistics show a correlation between the degree of seriousness of a failure and whether a design error was involved, at least part of this correlation is due to bias in data collection. The reporting and classification habits of the incident reporters have a strong effect on the data, a problem which is difficult to acoid for a general purpose data bank of the kind used. For example the data include some ROE reports, and this include a high proportion of design and common mode failures, since one of their objectives is to inform about new failure modes.

Judgement of what constitutes a 'serious incident' may be biassed, because the eventual consequence of each failure could in some cases only be guessed.

When system failure rates are estimated from component failure data, the results are in principle based on equipment failures alone. Statistics of the kind produced here, and in the Safety Related occurrences reports, can be used to provide a multiplication factor, which in turn can be used to give a crude estimate of the failure from all types of data. The correlations produced here suggest that a different factor should be used depending on whether all incidents are concerned, or only serious incidents. However most of the available equipment failure rate data is already biassed to some extent, in that a proportion of design, installation and fabrication faults, are included.

Discussion

The statistical study provides an indication that design errors might be more significant than their number suggests, because from the data collected 'serious' incidents are more strongly associated with design errors than with equipment failures. Equipment failures are used almost exclusively in judging the cost and consequences of failure for process plant. However, the data should be viewed with care. There are many sources of bias in the data collection process, and the results should be regarded as an indication of a possible association, rather than as evidence for a definite association.

	Design		Equipment	
	Number	%	Number	%
Serious	24	65%	11	22%
Not	13	35%	40	88%

Table 8

A surprisingly high number of design errors were not discovered until operation of plant. This may mean that there are many errors which are discovered during construction and commissioning, but are not considered to have safety significance, and are not reported.

Stage at which fault was discovered for design errors

Early commissioning	4	11 %
Late commissioning	1	3 %
Operation	21	57 %
Maintenance	8	22 %
Post maintenance testing	3	8 %

Table 9

Many of the errors, especially the 'oversight' errors, could have been prevented by simple checks in computer aided design programs if such had been used. Unfortunately, no data was available on the rôle played by information dissemination (or lack of it) in design errors, and so it proved impossible to determine how far improved information systems could help in reducing design errors.

That oversight and calculation errors are significant, is shown by the following table.

Design errors

Complex system	9
Unknown phenomena	6
Oversight	12
Inter disciplinary	1
Calculation	10

Note: Some incidents have several causes. Classification is subjective (on the part of the author). Errors due to design team communication problems could not be recorded.

Table 10

Calculation errors seem to be more serious than other types, though the size of statistical sample is too low, and there are too many sources of bias, to draw firm conclusions

Design error type	Serious	Not serious
Complex system	4	5
Unknown phenomenon	3	3
Oversight	7	5
Interdisciplinary	1	
Calculation	9	1

Table 11

Since a design objective is to avoid common failure modes, the concept of a 'common mode random component failure' does not exist. The one apparent exception to this rule, shown in the tables, with accession number 60093, is interesting. Several pipes were affected by stress corrosion cracking. Since the true cause of these failures could not be identified, at the time of the incidents, but the design was not changed, the failures must be accepted as common mode equipment failures.

That common mode effects are relatively common in association with design errors, is shown by the following table.

Common mode failures

	Common mode failure	Simple mode failure
Design errors	10	27
	27%	73%

Table 12

Design errors appear to be contributors to a sequence of failures, with safety consequences, rather than sole causes of failure, in most cases.

Multiple causes

	Single cause	Multiple cause
Design errors	7	30
	19%	81%

Table 13

Turning to specific failure modes, control rod and shut down rod timing is one frequent problem. From the original records it can be seen that this is a recognised problem, with no simple avoidanceprocedure.

A large proportion of the faults were circuit faults, (∿10%) which should be amenable to sneak path analysis, especially if this could be extended to take account of noise effects.

Of the design faults a large proportion involved jams and blockages (∿20%). An analysis similar to sneak path analysis, or cause consequence analysis, but in terms of mechanical or hydraulic linkages, would prove very useful here.

Another large group of design faults involved instrument adjustment and mechanical setting (∿8%). These are problems generally involved with comissioning, and are difficult to deal with on new plant. In most cases additional test procedures to confirm design assumptions, and some improved communication between design and commissioning engineers would be required to reduce the frequency of this type of error.

A good deal of investigation would have to be done, to determine if any worthwhile improvements could be achieved at reasonable cost.

Control oscillations represent about 5% of the design problems and confirm the value of 'plant simulation'. Extensions of the usual simulations, to include erroneous valve opening and blockage would appear to be very relevant.

In all, safety incidents due to design error appears to be about as frequent as safety incidents due to wear, corrosion, and similar unavoidable mechanisms. This is a tribute to the high standard of component reliability achieved in process plant. However, it also poses a problem, since conventional techniques are not so useful in reducing the problems of design errors. Also, design errors tend to be more serious than simple hardware failures.

Statistical Study II

The first study of abnormal occurrences in nuclear power plant (Statistical study I) showed that design errors are significant in determining overall plant reliability. However, it was felt that the results might be unduly pessimistic, because data from construction and operation were treated together. For that reason, in this second study, as a first step all abnormal occurrences reported for two nuclear power plants during one year of operation, were studied and classified.

Once again it proved difficult to determine how significant the incidents were, from a safety point of view, and in any case, the number of really significant incidents in two power stations during one year would be too low to provide a representative picture.

The USAEC's definition of Directly Significant Events (USAEC office of operations evaluation, Summary of abnormal occurrences reported to the Atomic Energy Commission during 1973, OOE-OS-001) provides good criteria for significance of an incident -

1) The release of radioactive materials from the site is in excess of limits set forth in Technical Specifications.

2) Significant property damage or personal injury.

3) Violation of a safety limit (on process variable values) set forth in technical specifications.

These criteria also have the advantage of being easy to apply. However, for completeness, a further criterion would have to be added

4) The probability of a very significant or catastrophic incident was raised significantly.

This criterion is very difficult to apply without detailed plant knowledge, and also access to fault tree analyses for each plant.

To overcome this problem of finding adequate records of significant events, in a further part of this study, group of events selected by the USAEC as worthwhile reporting in their 'Reactor Operating Experiences' bulletins, was used as a sample of 'significant' incidents. The sampling process involved has many disadvantages from the point of view of statistical study, but it

gives convenient access to a group of incidents which are considered significant. The records for 1972 were classified and recorded. Only incidents in light water power reactors were considered relevant.

The classification of incident causes is similar to that given earlier.

Table 14. Incident causes

Cause		Cause subclass	
C	Random component failure.....	M	Mechanical
		E	Electrical
D	Design error.....	U	Unknown phenomenon
		C	Complex system effects
		I	Interdisciplinary problem
		O	Oversight
		K	Communication problem
		Z	Calculation, sizing error
		S	Component selection error
P	Procedure error		
I	Installation error		
F	Fabrication fault		
M	Maintenance error		
O	Operator error		

A failure was classified as a random component failure if it was of a type known and accepted by engineers as inevitable in normal engineering practice, or if the cause could not be identified sufficiently closely to prevent future failure. Normal bearing wear, relay contact wear, aging effects on transistors, are all examples of this kind of failure. Design errors once again include problems due to effects unknown at design time, but which can be prevented in the light of experience. The criteria for classification as a design error are

a) The designer acknowledges the error, or

b) The design is changed after the failure, or

c) The same failure occurs repeatedly, at a frequency which is obviously unacceptable.

A new subclass, component selection errors, was introduced in view of the frequency of this kind of error. It is defined as errors which result in using a component in an unsuitable environment.

Procedure errors are a new class, similar to design errors. A procedure error was deemed to have occurred if

a) A procedure error was acknowledged, or

b) Procedures were changed after the failure.

Fabrication faults were recorded in those cases where the cause of the error was acknowledged to be in component manufacture. (Such faults might have many causes, mechanical, human, or even design of the manufacturing process).

Operator errors were recorded where the operator departed from correct operating procedure, or where operating procedures were non existent, and the operators actions led directly to failure.

A new procedure was used for recording incidents with multiple causes. Each cause is recorded separately, with all the causes for an incident recorded in one sequence. Initial and contributory causes are distinguished, and also whether the individual failures are latent or immediate. A latent failure is one for which the effect occurs some time after the failure, in response to some event independent of the failure. For example, shut down relay failure may not be noticed until a situation requiring shut down occurs.

As an attempt to get some indication of potential seriousness or otherwise of each incident, the stage at which the incident was observed was recorded. Only two stages were involved, operation (OP) and surveillance testing (SUR). It was also recorded whether the reactor was operating at power for the operational incidents (P). To distinguish between incidents occurring during surveillance testing, but resulting in unwanted consequences, it was recorded whether each incident was 'actual' (A) or found under test (T). 'Actual' failures are those for which the consequences occur, instead of being prevented by testing.

To guard against excessive pessimism with respect to common mode failures, both common mode effects and common mode consequences were recorded. A common mode effect was deemed to be involved if several components, assumed to be independent, were affected by the

same failure cause sufficiently to show some marks of the effect. A common mode consequence was deemed to have occurred, if the common mode effect resulted in failure to function in more than one component.

For the cause classes, a 1 indicates that either one of the indicated classes might have been correct. A comma between classification symbols indicates that both types of cause were involved.

Table 15. Incident characteristic codes

OP	Occured during operation
SUR	Occured during surveillance testing
P	Operation at power
A	Actual incident
T	Failure found under test
R	Revealed,immediate
UR	Unrevealed, latent

Table 15. DOCKET REPORTS OF ABNORMAL AND UNUSUAL OCCURRENCES (+ REPORTABLE INCIDENTS) FOR TWO REACTORS 1972

DOCKET NUMBER	REACTOR	DATE	REACTOR AGE (FROM OP.LICENSE)	STAGE AT WHICH INCIDENT DISCOV.	SERIOUS Y / NOT SERIOUS N	CAUSE	CAUSE SUBCLASS	MULTIPLE CAUSE Y / N	INITIAL CONTRIBUTORY CON / IN	COMMON MODE EFFECT Y / N	ONE TYPE COMP. 1 / MORE THAN ONE M	COMMON MODE CONSEQUENCE Y / N	INVALID R / UNINVALID U	FOUND UNDER TEST ACTUAL A	DESCRIPTION
50-237- -236, 240	DRESDEN 2	27/5/72		SUR P	N	D	C	N	IN	Y	1	N	U	T	Turbine stop valve limit switch would not activate protection relays on slow closure of stop valve
-239		20/3/72		UNSP	N	O		N	IN				U	T	Mode switch at 'refuel' but not locked
-241,		17/6/72		SUR	N	C	M	N	IN	Y	1	Y	U	T	Primary containment sample return valves binding
-245		15/6/72		SUR	Y	D	S	N	IN	Y	1	Y	U	T	Pressure switch drift
		18/6/72		SUR	Y	D	S	N	IN	N			U	T	Pressure switch drift
-246		26/6/72		SUR P	N	O		Y	CON	N			R	A	Pump trip not noted by operator stack gas recording omitted 8 hours
-250, 253		24/6/72		OP P	Y	I		N	IN	N			R	A	Loose wires in standby diesel gen.

DOCKET REPORTS

DOCKET NUMBER	REACTOR	DATE	REACTOR AGE (FROM OP. LICENSE)	STAGE AT WHICH INCIDENT DETECTED	SERIOUS NOT SERIOUS Y N	CAUSE	CAUSE SUBCLASS	MULTIPLE CAUSE Y N	INITIAL CONTRIBUTORY CON	COMMON MODE EFFECT Y N	ONE TYPE COMP. MORE THAN ONE 1 M	COMMON MODE CONSEQUENCE Y N	REVEALED UNREVEALED R U	ACTUAL FOUND UNDER TESTT A	DESCRIPTION
256, 264	DRESDEN 2	27/6/72		SUR	Y	D	U	N		Y	1	Y	U	T	Electro hydrolic pressure switc drift, as before
258, 268		29/8/72		OP P	Y	I,D	U,Z	N		Y	1	N	R	A	Flow restrictor cone welds brok - new stop pins fitted
263		8/9/72		SUR	Y	D	S	N		Y	1	Y	U	T	2 Reactor vessel high press switch drift
265		19/9/72		SUR	Y	D	S	N		Y	1	Y	U	T	Low press permissive p.s.w.drif
266		3/9/72		OP P	Y	C,D	?			Y	1	N	R	A	Timer relay in generator starte drifted
270, 271		25/10/72		SUR	Y	D	S	N		Y	1	Y	U	T	Low pressure switch drift
272		29/10/72		SUR	Y	C	M	N		N			U	T	MSV fast close control solenoid stuck-crud
274		29/10/72		SUR	Y	I		N		N			U	T	MSV fast close solenoid valve, conector broken
280, 282,		29/11/72		SUR	N	D		N		Y	1	Y	U	T	MS low press switches drifted again
284				This incident not used in statistical analysis to avoid double counting											
285		17/8/72		OP P	Y	P		N		N			R	A	Local rod witdrewal in unusual Yenon circumstances led to short period

DOCKET REPORTS

DOCKET NUMBER	REACTOR	DATE	REACTOR AGE (FROM OP. LICENSE)	STAGE AT WHICH INCIDENT	SERIOUS NOT SERIOUS Y N	CAUSE	CAUSE SUBCLASS	MULTIPLE CAUSE Y N	INITIAL CONTRIBUTORY CON	COMMON MODE EFFECT Y N	ONE TYPE COMP. MORE THAN ONE 1 M	COMMON MODE CONSEQUENCE Y N	REVEALED UNREVEALED R U	ACTUAL FOUND UNDER TESTT A	DESCRIPTION
50-237-209	DRESDEN 2			SUR	N	D	C	N	IN	Y	1	N	U	T	Main steam line high flow isolation switch rusted - dripping water - solution - seal switche
-211				SUR	Y	I/R		N	IN	N			U	T	LPCI valve jammed - torgue limi switch adjustment - motor over-heated
-218, 221		25/2/72		OP S	N	C	M	N	IN	N			R	A	Interlock on fuelling platform - limit switch destroyed - no interlock effect
-226		2/3/72		SUR	Y	?		N	IN	N			U	T	Defective dieselgenerator air starter motor
-227		5/3/72		SUR	Y	C	E	N	IN	N			U	T	LPCT pump motor circuit breakes dirty
-228, 231		/3/72		SUR	Y	D	U	N	IN	Y	1	Y	U	T	Flow switch paddle broken, lost Screws vibrated loose
-229		24/3/72		MN	Y	P	K	N	IN	Y	M	Y	R	A	Maintenance procedure on transformer inactivated S/by gas treatment, core spray etc.
-233		17/5/72		OP	Y	P	O/K	N	IN	N			R	A	High waste tank activity due to blowdown - valve position wrong
-235				SUR	Y	C,D	U,S	Y	IN	Y	4	Y	R	T	Seals on reactor containment leaking

DOCKET NUMBER	REACTOR	DATE	REACTOR AGE (FROM OP.LICENSE)	STAGE AT WHICH INCIDENT DETECTED	SERIOUS Y / NOT SERIOUS N	CAUSE	CAUSE SUBCLASS	MULTIPLE CAUSE Y / N	INITIAL CONTRIBUTORY CON. Y / N	COMMON MODE EFFECT Y / N	ONE TYPE COMP. 1 / MORE THAN ONE M	COMMON MODE CONSEQUENCE Y / N	REVEALED R / UNREVEALED U	ACTUAL A / FOUND UNDER TESTT	DESCRIPTION
50-237 290	DRESDEN 2	1/12/72		PM	Y	D	O,S	N		Y	1	N	U	T	HPCI valve actuator solenoid valve - 125 V coil in 250 V circuit

DOCKET NUMBER	REACTOR	DATE	REACTOR AGE (FROM OP.LICENSE)	STAGE AT WHICH INCIDENT DISCOV.	SERIOUS Y / NOT SERIOUS N	CAUSE	CAUSE SUBCLASS	MULTIPLE CAUSE Y / N	INITIAL CONTRIBUTORY CON.	COMMON MODE EFFECT Y / N	ONE TYPE COMP. 1 / MORE THAN ONE M	COMMON MODE CONSEQUENCE Y / N	REVEALED R / UNREVEALED U	ACTUAL A / FOUND UNDER TESTT	DESCRIPTION
50-263	Monticello														
103		15/1/72		SUR	N	I		N		N			U	T	Shut down solenoid interfered with reset opening accumulator
104		20/1/72		SUR	Y	D	U	H		Y	1	N	U	T	HPCI actvator. Jam nut turned, new fixing method
106		24/1/72		OP P	N	D	C,Z	N		N			R	A	Core flux colibration error - underestimate of peaking in computer program
113, 118				SUR	N	D	U	N		Y	1	Y	U	T	Design of flow measurement taps needed changing - testing at high main steam flow prevented HCPI activation
116		1/3/72		SUR	Y	D/C	?	N		Y	1	Y			RCIC high steam flow isolation switch set point wrong - too much play in link, machined
119		28/3/72		SUR	N	M		N		N			U	T	Service water regulating valve actuating signal reversed
		3/4/72		SUR	Y	P/C		N		N			U	T	Manual back seating valve caused unidentified actuator clutch failure
		3/4/72		SUR	N	P		N		Y	1	Y	U	T	Test procedure prevented identification of whether failed component was operational component or spare

DOCKET REPORTS

DOCKET NUMBER	REACTOR	DATE	REACTOR AGE (FROM OP. LICENSE)	STAGE AT WHICH INCIDENT DISCOV.	SERIOUS NOT SERIOUS Y N	CAUSE	CAUSE SUBCLASS	MULTIPLE CAUSE Y N	INITIAL CONTRIBUTORY CON. IN	COMMON MODE EFFECT Y N	ONE TYPE COMP. MORE THAN ONE 1 M	COMMON MODE CONSEQUENCE Y N	REVEALED UNREVEALED R U	ACTUAL FOUND UNDER TEST A	DESCRIPTION
50-263	Monticello														
123		14/5/72		OP P	N	D	C	N		N			R	A	APRM 4% calibration error - unusual flux distribution
124		1/5/72		OP P	N	C	E	N		N			R	A	13.8 KV core phase fault
125		26/2/72		SUR P	N	C	E	Y	IN	Y	1	Y	R	A	During surveillance test, 4 turbine stop valves tripped
					Y	?		Y	CON	N			UR	A	Both relief and 2 safety valve opened. Drywell pressurisation
					Y	D	C	Y	CON	Y	1	Y	UR	A	Bypass valves could not open because 110% open control valve even though stop valves were closed
					Y	D	C	Y	CON	Y	M	Y	UR	A	Sagety valve jet displaced cabl tray
128		13/5/72		SUR	N	C	M	N		N			UR	T	Contactor to isolation valve not or jammed
130		23/5/72		OP P	Y	C	M	N		N			UR	T	Seal leakage in control rod hydraulic controller
132		20/6/72		OP P	N	C	E	Y	CON	N			R	A	Stackgas sampler tripped, no alarm due to bad connection
133		14/6/72		SUR	N	D	Z	N		N	1	Y	UR	T	RHR service water pump not delivering required head + better flow matering. Tech spec change

DOCKET REPORTS

DOCKET NUMBER	REACTOR	DATE	REACTOR AGE (FROM OP. LICENSE)	STAGE AT WHICH INCIDENT DISCOV.	SERIOUS NOT SERIOUS Y N	CAUSE	CAUSE SUBCLASS	MULTIPLE CAUSE Y N	INITIAL CONTRIBUTORY CON. IN	COMMON MODE EFFECT Y N	ONE TYPE COMP. MORE THAN ONE 1 M	COMMON MODE CONSEQUENCE Y N	REVEALED UNREVEALED R U	ACTUAL FOUND UNDER TEST A	DESCRIPTION
50-236	Monticello														
-137		10/7/72		OP P	N	I		Y	IN	N			R	A	Poorly soldered transistor in generator field control + turbine trip
				OP P	Y	C	M		CON	N		N	UR	A	Rust prevented relief valve pilot closing
				OP P	Y	?			CON	N	1		UR	A	One relief valve did not open
				OP P	Y	?			CON	Y		Y	UR	A	Twc safety valves opened prematurely
				OP P	N	I			CON	Y	1	Y	UR	A	Tape over pressure taps on Drywell
139		17/7/72		SUR P	Y	C	M	Y	IN	N			UR	T	HCPI stop check valve pin, broken, lodged
				SUR	Y	D	C	Y	CON	N			UR	A	Rupture disc burst, relief pressure. Sensors too slow
				SUR	N	D	C	Y	CON	Y	M	Y	UR	A	Rupture disc steam damaged steam leak detection temp. switches
140		21/7/72		OP P	N	C	E	Y	IN	N			R	A	Short circuit started transformer deluge system
					N	C	M	Y	CON	N			UR	A	Control rod hydraulic control seal leak
					Y	D	?	N	CON	N			UR	A	Safety value dis not open

DOCKET REPORTS

DOCKET NUMBER	REACTOR	DATE	REACTOR AGE (FROM OP. LICENSE)	STAGE AT WHICH INCIDENT DISCOV.	SERIOUS NOT SERIOUS Y N	CAUSE	CAUSE SUBCLASS	MULTIPLE CAUSE Y N	INITIAL CONTRIBUTORY CON IN	COMMON MODE EFFECT Y N	ONE TYPE COMP. MORE THAN ONE 1 M	COMMON MODE CONSEQUENCE Y N	REVEALED UNREVEALED R U	ACTUAL FOUND UNDER TEST A	DESCRIPTION
50-236	Monticello														
143		21/7/72		OP P	N	P		N		N			R	A	Procedure for ARPM calibration in error
142		27/7/72		SUR P	Y	C	M	N		N			R	A	HCPI
143		31/7/72		SUR	Y	I		N		N			R	A	HPCI turbine control valve contained plastic pipe cap
153		31/8/72		SUR	Y	D	S	N		Y	1	Y	R	A	4 Pecco switches
147		28/7/72		OP	N	O		Y	IN	N			R	A	Operator turned mode switch to RUN instead of STARTUP
				OP	N	I		Y	CON	N			UR	A	Loose screws on isolator motor contactor prevented valve closure
155		15/8/72		SUR	N	C	M	N		N			R	A	Rust in head orifix of air rela caused delay in starting diesel also 'spurious' alarm
160		7/11/72		SUR	N	C	M	N		N			UR	T	Failure of diff.pressure switch bellows on building/torus vacuum breaker

DOCKET REPORTS

DOCKET NUMBER	REACTOR	DATE	REACTOR AGE (FROM OP. LICENSE)	STAGE AT WHICH INCIDENT DISCOV.	SERIOUS NOT SERIOUS Y N	CAUSE	CAUSE SUBCLASS	MULTIPLE CAUSE Y N	INITIAL CONTRIBUTORY CON IN	COMMON MODE EFFECT Y N	ONE TYPE COMP. MORE THAN ONE 1 M	COMMON MODE CONSEQUENCE Y N	REVEALED UNREVEALED R U	ACTUAL FOUND UNDER TEST A	DESCRIPTION
50-236 -160	Monticello	20/9/73		OP P	N	I		N		N			R	A	Boot seal on terms vacuum breake butterfly valve not inflated - excessive dearance on pilot valve actuator
168		16/12/72		OP P	N	D	O,C	N		Y	1	N	R	A	RHR pump motor air deflector crack + damage, shorting in pump coil. New design
191, 168, 174		15,19/12/72		SUR	Y	D	U	N		Y	1	Y	UR	T	Teflon packing in butterfly valve (vacuum breaker) glands outgassed + sticking
				SUR	Y	D	U	N		Y	1	Y	UR	T	Non dosure could not be indicate - new contact switch design required
172, 205		15/12/72		OP	N	D	C	N		Y	1	N	R	A	At low flow, river water forced dirt into RHR service water pump glands
171, 172				SUR	Y	I		N		Y	1	Y	UR	T	Torus suction ring Langer supports all were weak

Table 16. REACTOR OPERATING EXPERIENCE REPORTS 1972

BULLETIN NO.	REACTOR	DATE	REACTOR AGE (FROM OP.LICENCE)	STAGE AT WHICH INCIDENT DISCOV.	SERIOUS NOT SERIOUS	CAUSE	CAUSE SUBCLASS	MULTIPLE CAUSE	INITIAL CONTRIBUTORY CON	COMMON MODE EFFECT	ONE TYPE COMP. 1 MANY M	COMMON MODE CONSEQUENCE	REVEALED UNREVEALED R UR	ACTUAL FOUND UNDER TESTT A	DESCRIPTION
72-1				OP		C,D	M,Z	N		N			R	A	Fuel handling grapple spring became 'set' dropped fuel ont core support plate - new spri design
				OP		C,D	M,U	N		N			R	A	Galling on fuel prevented pro grapple seating, dropped fuel microswitch check installed
				OP		C,D	E,C	N		Y	1	N	R	A	Relay contacts welded due to vibration, caused uncontrolle raising of irradiated fuel. H suppression + interlock fitte
72-3				MN		D	Z	N		N			R	A	Strainer torn in pieces by surges, turbulence
72-4				SUR?		D	Z	Y	CON	Y	1	N	UR		Manual shutdown could displace a pin in govern or linkage - oversize
						P		Y	IN	1	1	N	UR		Pin fitted, new operating pro-cedure
				SUR?		D	O	N		N			UR		Air start motor solenoid valve jammed - air supply taken from wrong side of lubricator
						C	M	N		Y	1	Y	R		Weld slag in air starter motor supply line
						C	M	N		N			R		Air starter motor cylinder bro ken
				SUR?		D	C	N		N			UR		Grozen fuel priming pump
				SUR?		D	C	N		N			UR		Timing of hydraulic governor c in too late - pressure switch wrongly sited, moved

REACTOR OPERATING EXPERIENCE REPORTS 1972

BULLETIN NO.	REACTOR	DATE	REACTOR AGE (FROM OP.LICENCE)	STAGE AT WHICH INCIDENT DISCOV.	SERIOUS NOT SERIOUS	CAUSE	CAUSE SUBCLASS	MULTIPLE CAUSE	INITIAL CONTRIBUTORY CON	COMMON MODE EFFECT	ONE TYPE COMP. 1 MANY M	COMMON MODE CONSEQUENCE	REVEALED UNREVEALED R UR	ACTUAL FOUND UNDER TESTT A	DESCRIPTION
72-4				SUR?		C,P	M	N		Y	M	Y	R		Rust in air starter motor supp
				SUR		D	C	N		N			UR	T	Drop in oil pressure raised ir relevant alarm
						D	O,U	N		N			R		Hydraulic accumulator tube failed, replaced with flexible coupling
				SUR		C	M	Y	IN	N			UR	T	Dirty fuel, and operator had
						O							R	T	not reset overspeed trip
						D	Z	N		N			R	?	Generator rotor balance weight bolts sheared
				SUR?		?		N		Y	1	Y	R	?	Two diodes in exciter failed
						O		N		N			R		Diesel generator speed not reset after shut down
				OP		?		Y	IN	N			R	A	Diesel coolant pump failed
						D	C	Y	CON	N			R	A	Coolant boost pump could not start - static pressure pre-vented low pressure actuation og boost pump - circuit modifi
				OP		D	C	N		N			R	A	Warm weather activated cut out interlock circuits
						D	O	N		N			R	A	Lubrication oil supply line to long. Low pressure in cold weather prevented start

REACTOR OPERATING EXPERIENCE REPORTS 1972

BULLETIN NO.	REACTOR	DATE	REACTOR AGE (FROM OP.LICENCE)	STAGE AT WHICH INCIDENT DISCOV.	SERIOUS NOT SERIOUS	CAUSE	CAUSE SUBCLASS	MULTIPLE CAUSE	INITIAL CONTRIBUTORY IN CON	COMMON MODE EFFECT	ONE TYPE COMP. 1 MANY M	COMMON MODE CONSEQUENCE	REVEALED UNREVEALED R UR	ACTUAL FOUND UNDER TEST A	DESCRIPTION
72-4				OP		C	E	Y	CON	N			UR	A	Power supply loss - fuse blow prevented start of gas turbir
						C	E	Y	CON	N			UR	A	Cause of blown fuse was loose relay terminal - short circui
				OP		I		Y		N			UR	A	Tube oil pump motor brush rig position wrong
						I		Y		N			UR	A	Tube oil temp set point too l
				OP?		D	Z	N		N			UR		Tube oil heaters undersized
						M		N		N			UR		Forgot? to reinstall tube oil reservoir vent line
				?		C	M	N		Y	1	Y	UR		Gas turbine air start motor seal leaks
				OP		O		N		N			R	A	Oil pump switch in 'hand' pos ition, caused oil to be ex- pelled from system

REACTOR OPERATING EXPERIENCE REPORTS 1972

BULLETIN NO.	REACTOR	DATE	REACTOR AGE (FROM OP.LICENCE)	STAGE AT WHICH INCIDENT DISCOV.	SERIOUS NOT SERIOUS	CAUSE	CAUSE SUBCLASS	MULTIPLE CAUSE	INITIAL CONTRIBUTORY IN CON	COMMON MODE EFFECT	ONE TYPE COMP. 1 MANY M	COMMON MODE CONSEQUENCE	REVEALED UNREVEALED R UR	ACTUAL FOUND UNDER TEST A	DESCRIPTION
72-5				SUR		O		Y	IN	N			R	A	During test, battery driven oi pump was not stopped. Depleted battery
						D	C	Y	CON	Y	M	Y	UR	A	Loss of DC Power caused reacto then turbine trip, prevented switch to emergency power - lubrication lost. Turbine siez
72-6				OP		D	O,Z	N		N			R	A	Low air flow in instrument air dryer - heater ignited filter paper, melted, silver soldered air header
				OP		D	O,U	N		N			R	A	Short circuit in charcoal filt heater
				OP		C	M	N	IN	N			R	A	Oil leak from pump motor beari thermo couple junction box. Dripped onto hot pipe
				OP		C,D	O,C	N		N			R	A	High pressure oil line rupture seeped onto hot oil volute. Replaced by new design
72-7				SUR		C	E	Y	IN	N			R	A	After surveillance trip, recir
						C	M	Y	IN	N			UR	A	culation pumps would not re-
						I		Y	IN	N			UR	A	start, one due to limit switch
						C	M	Y	CON	N			UR	A	failure, the other due to time
						D	C	Y	CON	Y	1	N	UR	A	delay inaladjustment and pres- sure switch drift. Seals were damaged because the pumps coul not be isolated. RHR a isolati valves failed

REACTOR OPERATING EXPERIENCE REPORTS 1972

BULLETIN NO.	REACTOR	DATE	REACTOR AGE (FROM OP.LICENCE)	STAGE AT WHICH INCIDENT DISCOV.	SERIOUS NOT SERIOUS	CAUSE	CAUSE SUBCLASS	MULTIPLE CAUSE	INITIAL CONTRIBUTORY CON	COMMON MODE EFFECT	ONE TYPE COMP. 1 MANY M	COMMON MODE CONSEQUENCE	REVEALED UNREVEALED R UR	ACTUAL FOUND UNDER TESTT A	DESCRIPTION
72-7						D	C	Y	CON	N			UR	A	Valve failures
						C		Y	CON	N			UR	A	
						I		Y	CON	Y	1	Y	UR	A	Torque switches on pump isolation valves wrongly set
72-8				SUR		D	C	N		Y	1	Y	UR	A	Torus baffles displaced by safety valve line air compression, displacing torus water
						D	C	Y	CON	Y	1	Y	UR	A	Baffle damage brok vacuum breaker valve air line
72-9				IN		C	E	Y	IN	N			R	A	Shott circuit
						P		Y	CON	N			R	A	Plub overload test procedure, cause destruction of heater control components
						C	M			Y	1	Y	R	A	Damper binding caused exhaust of containent air to stack
						D	K,C	N		Y	1	Y	UR	A	Control wiring error to dampe
						C	E	N		N			UR	A	Damaged FET in
72-11				OP		MN	E	Y	IN	N			UR	A	Offsite substation trip, arci
						D	C	Y	CON	Y	M	Y	UR	A	Protective relay delays were too long, gave generator over current trip
						C	E	Y	CON	N			UR	A	Main generator breaker timing failed - SCR short

REACTOR OPERATING EXPERIENCE REPORTS 1972

BULLETIN	REACTOR	DATE	REACTOR AGE (FROM OP.LICENCE)	STAGE AT WHICH INCIDENT DISCOV.	SERIOUS NOT SERIOUS	CAUSE	CAUSE SUBCLASS	MULTIPLE CAUSE	INITIAL CONTRIBUTORY CON	COMMON MODE EFFECT	ONE TYPE COMP. 1 MANY M	COMMON MODE CONSEQUENCE	REVEALED UNREVEALED R UR	ACTUAL FOUND UNDER TESTT A	DESCRIPTION
72-11						M		Y	CON	N			UR	A	Remote control wiring disconnected from circuit breaker - omission after maintenance
						M		Y	CON	N			UR	A	Torque switch setting on emergency condensate return valve too highly valve jammed
						P		Y	CON						Operators had no procedure for this circumstance - would have allowed full blowdown - senior engineer stopped it
						D	O	Y	CON	Y	M	Y	UR	A	Loss of instrumentation, no emergency power
						C,D	J	Y	CON	N			UR	A	Safety valve tripped, bellows ruptured
						D	O	Y	CON	Y	M	Y	R	A	Dry well cooling fans crud pumps triplet, had no auto restart for emergency power
72-12				SUR		C,F	M,C	N		Y	1	Y	R	A	Stress corrosion cracking of turbine bucket pins - Cutting oil contamination
				OP P		F		N		N			R	A	Weld penetration deficient on level controller of turbine steam reheater - broke. Radiation exposure

BULLETIN NO.	REACTOR	DATE	REACTOR AGE (FROM OP.LICENCE)	STAGE AT WHICH INCIDENT DISCOV.	SERIOUS NOT SERIOUS	CAUSE	CAUSE SUBCLASS	MULTIPLE CAUSE	INITIAL CONTRIBUTORY	IN CON	COMMON MODE EFFECT	ONE TYPE COMP. 1 MANY	COMMON MODE CONSEQUENCE	REVEALED UNREVEALED	R UR	ACTUAL FOUND UNDER TEST?	A	DESCRIPTION
72-13				OP		C	M	Y	IN		N			R		A		Turbine control dadpot vibrat loose
						D	C	Y	CON		Y	M	Y	UR				This caused instability, vibr tion, damaging other componen
						C	M	Y	CON		N			R		A		Relief valve opened early (spring relaxation), would no close (erosion)
						D	K,S	Y	CON		Y	1	Y	R		A		Pilot valves of relief valve not designed for environment
72-14				OP		C	M	Y	IN		N			R		A		Condensate looster pump trip, causing two feed pumps to trij - low NPSH. Reactor tripped
						D	C	Y	CON		N			UR		A		Feedwater manual control locke
						D	U	Y	CON		N			R		A		out by low pressure due to rapid close demand isolation valve stalled, high differenti pressure
						C	M	Y	CON		N			R		A		Safety valve opened early, pressurising containment, acti ating ECCS.
						D	C	Y	CON		N			UR		A		Safety valve jet damaged relie valve
						P		Y	CON		N			UR		A		Feedwater level control proce- dures revised

BULLETIN NO.	REACTOR	DATE	REACTOR AGE (FROM OP.LICENCE)	STAGE AT WHICH INCIDENT DISCOV.	SERIOUS NOT SERIOUS	CAUSE	CAUSE SUBCLASS	MULTIPLE CAUSE	INITIAL CONTRIBUTORY	IN CON	COMMON MODE EFFECT	ONE TYPE COMP. 1 MANY	COMMON MODE CONSEQUENCE	REVEALED UNREVEALED	R UR	ACTUAL FOUND UNDER TEST?	A	DESCRIPTION
72-15				EC		D	O	Y	IN		N			R		A		Failure of safety valve header during hot functional test - Designer had not allowed for dynamic forces
						D	C	Y	CON		Y	M	Y	R		A		Many structural components, some valves, damaged, pressure transmitters destroyed
				This incident occurred during commissioning, Not counted in statistics														
72-18				SUR		M		N			Y	1	Y	UR		T		Epoxy flowed onto control rod magnetic clutch
				SUR		D/P		N			Y	1	Y	UR		T		Control rod energy absorbing dash pots, when unfilled, did not absorb energy. This led to damage and non performance
				OP		D	C	N			Y	1	N	R		A		Control rod motor dutch drag- ging led to intermittent CRP malfunction
				SUR		D	U	Y	IN		M			R		A		Loose dowel pins caused gallin of clutch
				LC?		D	C	Y	CON		Y	M	Y	UR		A		Alarm signals could not respon quickly enough
						C	M	Y	CON		N			UR		A		Motor clutch slip

BULLETIN NO.	REACTOR	DATE	REACTOR AGE (FROM OP. LICENCE)	STAGE AT WHICH INCIDENT DISCOV.	SERIOUS NOT SERIOUS	CAUSE	CAUSE SUBCLASS	MULTIPLE CAUSE	INITIAL CONTRIBUTORY CON	COMMON MODE EFFECT	ONE TYPE COMP. 1 MANY M	COMMON MODE CONSEQUENCE	REVEALED UNREVEALED R UR	FOUND UNDER TEST? ACTUAL A	DESCRIPTION
72-19				SUR		D	U,C	N		Y	1	Y	UR	T	Roller from CRD blade jammed CRD index tube. Suggested tha this was flow induced roller failure
				OP		C, P	M	N		Y	1	Y	R	A	Control rods did not fully insert. Grask hydraulic press insertion did not work due to piston leakage in last (low flow) grade. Increased testin
				OP		C, D	O	N		N			R	A	Control rod motor transformer short - Redesigned circuit wi fuses

Discussion II

The distribution of causes in the second statistical study still shows a heavy emphasis on design errors, as Table 17 shows. However, an effect which steels some light on the failure avoidance and design process, was observed in reading the original failure reports (Table 15). Whether a failure is classed as a design error or a random component failure depends on how difficult it is to determine the true cause of failure. With the opportunity to search further, there is a tendency to reclassify failures as design errors. This is especially true if several failures of the same kind occur, as there is then an opportunity to build up experience of causes, and an incentive for more thorough analysis of incidents.

Another effect is shown by the class of 'component selection' design errors. In most cases these failures were due to calibration shift in pressure switches. In many cases the direct cause was vibration. The cases classified as design errors were those in which the instruments were replaced by a different type, or a design modification was made to reduce the effects of vibration, etc.

Design	28	41%	oversight	2
			component selection	8
			complex system	10
			effect unknown at design time	7
			calculation error	3
Operator	3	4.4%		
Component	18	27%	mechanical	11
			electrical	5
Installation/maintenance	12	18%		
Procedure	5	7.4%	communication	2
			oversight	1
			complex system	2
Unknown	2	3%		
	68	100.8%		

Table 17. Distribution of causes of failure for two reactors during one year.

Design	43	46%	oversight	8
			component selection	1
			complex system effect	19
			effect unknown at design time	7
			calculation/ sizing error	6
			communication problem	2
Operator	4	4.3%		
Component	26	28%	mechanical	19
			electrical	7
Installation/ maintenance/ fabrication	11	12%		
Procedure	7	7.5%		
Unknown	2	2.2%		
	93	100%		

Table 18. Distribution of causes of failure - Reactor operating experiences 1972 (Power reactors).

Such failures can still, however, be regarded as equipment failures, or maybe should be regarded as a class for themselves. All but one of the 'component selection' failures could be regarded in this way, the proportion of such errors being 12% (remaining 'design error' failures form 29% of all failures).

Once again, it proved difficult to draw conclusions about the relative significance or seriousness of incidents. The 'Reactor Operating Experiences' reports were disappointing in this respect, since they include many incidents which are not too serious in themselves, but which are of a type which is relatively frequent. Table 18 gives the cause distribution for these incidents, although the results should be viewed with care, since it has not been possible for the author to determine the exact criteria for choice of these incidents.

One thing which is clear from the studies is that there are very few single failure incidents which are serious in themselves (as would be expected). There were surprisingly many incidents

involving many independent failures (Fig. 2 and 3). One would, a priori, expect the probability of multiple failures to be very low. Apparently, when one or two initial failures occur, they can bring the power plant into a state where several latent failures reveal themselves. This view is derived from some typical incidents and is supported by table 19 and fig. 2 and 3.

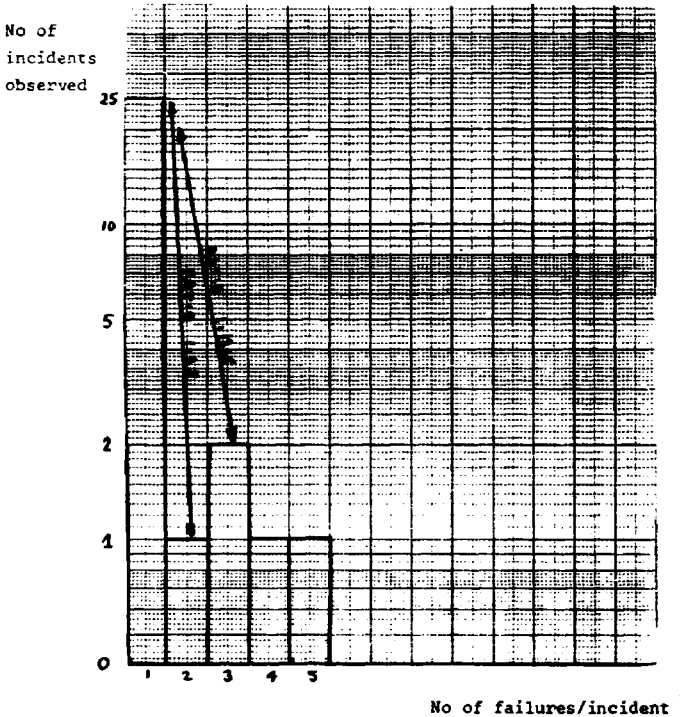
To give an example of the significance (and surprise) involved in table 2 and 3, consider a 'typical' failure rate of 0.01 per year, or 0.01 per activation for intermittently working components. The ratio of single failures to (say) six fold failures would, on a simple hypothesis be $0.01:(0.01)^6$, or $10^{10}:1$. Even with unrealistically high failure rates of 0.1, the ratio should be $10^5:1$, rather than approximately 25:1, as observed. There are several possible explanations of this discrepancy, all of which seem to be required.

1. Most of the single failures which occur are not in any way significant to safety, and are therefore not reported as abnormal occurrences. This effect might account for as much as one or two orders of magnitude, but not nine.

2. Safety systems and shut down systems are especially failure prone, in that they incorporate very large numbers of components. They are only brought into effect after at least one failure has occurred, and therefore will be responsible for a number of 'double failures'. This effect might again explain a difference of an order of magnitude, though one would still expect the ratio between double failures and higher order multiple failures to be several orders of magnitude larger than it is.

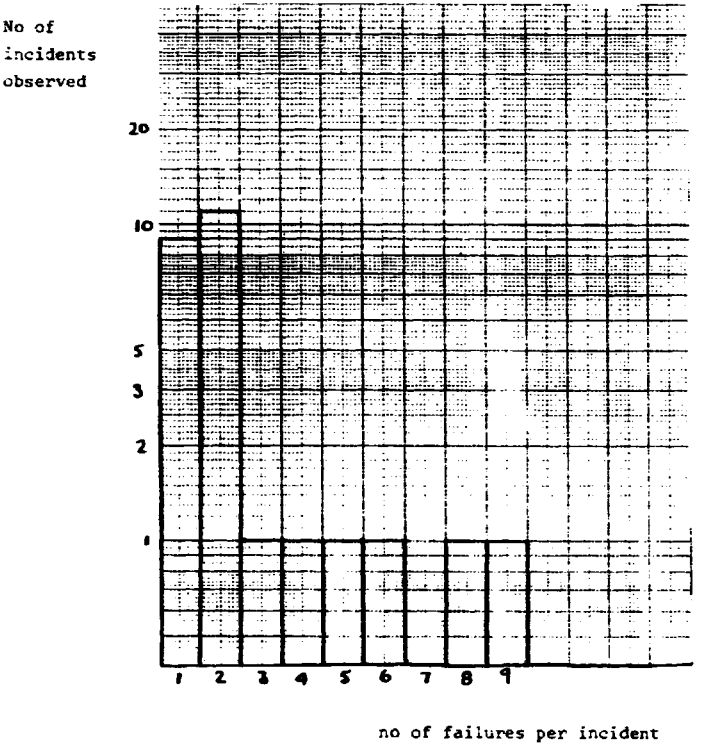
3. Safety systems are tested periodically, rather than continuously by use. Presumably the failure rates for intermittently operating systems are higher than for continuously operating systems in spite of high test frequencies. It is worth noting that maintenance and design errors are not usually considered in setting test frequencies.

4. For intermittently operating systems with complex event sequences, and particularly for safety systems, there are very many different operating situations to account for. This means that there are many different failure types to account



Note: Latent and unrevealed failures activated during incidents are regarded as independent.

Fig. 2. Histogram of number of 'actual' incidents involving several independent failures, for two operating reactors during one year.



Note: Latent and unrevealed failures, activated during incidents. are regarded as independent.

Fig. 3. Histogram of 'actual' incidents involving several independent failures. Incidents taken from ROE bulletins for 1972 Power reactors only.

for, for the later failures in a sequence. Design errors which are not detected during testing, usually require special circumstances for failure to result.

5. Common mode failures. (Though these cannot explain the large number of independent failures).

	initial	contributory	total
immediate/revealed	23	2	25
latent/unrevealed	1	11	12
	24	13	37

Table 19. Revealed/Immediate and unrevealed/latent failures, correlated with initial/contributory failures. (Two reactors during 1972). Operational or actual incidents only.

The number of incidents involving several independent failures was, as can be seen, quite high. Common mode failure effects were also fairly wide spread, as can be seen from table 20.

Failure cause	No common mode effect	Common mode effect. No common mode consequence	Common mode consequence
Design	5	7	14
26	19%	27%	54%
Operation	3	0	0
Component?*	14	1	4
Procedure	4		2
Installation/ maintenance	9		2
Total	35	8	22
65	54%	12%	34%

*Incidents were classified as component failures if no design modifications were made. Common mode failures would result in immediate modification, if the failures in themselves threatened safety and would hence be defined as design errors.

Table 20. Common mode effects for two reactors during one year.

The kind of effects involved in multiple failures, and explained in point four, can be illustrated by steam release incidents in boiling water reactors. A coupling of control and safety valve problems has lead in several cases to a release of steam and hot boiler water into containment. The new component environment has then revealed problems with cable, terminal and motor insulation, as well as containment isolation valve problems. To test a complete reactor in an atmosphere of steam and hot water would presumably be unrealistic, but it is this kind of changed environment which reveals problems.

Conclusions

One clear conclusion from these studies is that design errors are an important factor in nuclear power plant reliability. It seems likely that this is a consequence of the use of redundancy techniques, which in turn reduce the problems of random component failure. For anticipated failures the probabilities of serious consequences become vanishingly small. As the consequences of random component failure diminish, so the relative significance of design errors increases.

A. Ideally, a study of this kind would provide information for estimating the impact of design errors on reliability. In fact, part of the evidence was helpful in this way. For nuclear power plant abnormal occurrences, the ratio of 'design error failures' to random component failures, is reasonably constant. The value of the ratio lies between 1:1 and 1:4 normally. However, direct quantitative conclusions cannot be drawn, for the following (rather long) chain of reasons.

1. There is some evidence that more serious failures may be associated with design errors, but it is difficult to judge the size of this effect; to what extent it is due to prevalence of common mode failures among design errors; and to what extent it arises from the unusual (unpredictable) consequences of design errors.

2. The 'failure rate' data obtained from reliability data banks already contains some allowance for design errors, but the extent of this allowance is not usually known, and varies from component to component.

3. While the consequences of random failure are relatively easy to predict (because the models of failure are well known), the consequences of design error are in many cases very difficult to predict. If the type of design error were known to the 'reliability analyst', he would tell 'the designer', and the problem would disappear. This problem is especially associated with 'mis-wiring' design errors, or mis location of components, so that they affect each other adversely, or the use of incorrect design objectives.

4. While the problem of judging the consequences of design error are large in some cases, in many others, the failure

mechanism can be predicted. For example, component selection errors usually lead directly to 'non-functioning' failures.

The problems of estimating the effect of design error may eventually be solved by extending reliability analysis back to the design stage. On the other hand, it may prove easier simply to reduce the problem, so that design errors have an insignificant effect on reliability.

B. Some of the 'design errors' were encouraging, in that there is a clear route to reducing their number. 'Component selection' problems should be very significantly reduced by rapid feed back of failure data to design teams, by type testing, and by standardisation of components, as practised for Canadian, and with increasing thouroughness, for U.S. reactor systems.

C. 'Complex system' analysis techniques seem relevant to reducing the number of design errors, and possibly also the number of procedural errors. Sneak path analysis, cause consequence analysis, routeing analysis, and common mode failure analysis have a clear rôle to play. Development of systematic techniques for studying the effects of blockage and of hydraulic effects such as vibration and water hammer would be worthwhile.

D. Design errors resulting from unknown effects should be reduced significantly in frequency, as more experience is gained of standardised plant types.

E. One of the most significant findings in this study, was the unexpectedly high number of incidents involving several independent failures. These involved long sequences of events, with as many as nine independent failures involved. The rate of occurrence was several orders of magnitude larger than would be expected simply by multiplying together the necessary number of 'typical' failure rates.

Such multiple failures involved shut down sequences for the most part. They can be explained by the large number of different sequences under different failure conditions; the large number of components involved; and the number of unrevealed and latent errors which manage to avoid discovery during testing. These last can presumably be explained as failures arising due to unusual circumstances during shutdown, and design errors which only gradually show their effects. Operator errors played a rôle in many of the long sequences.

It is worth mentioning in this context that none of the incidents studied resulted in a design basis accident. Further, as far as the author could tell, in no case did any of the long sequences of failures bring the state of the plant significantly close to a design basis accident. It would be interesting to see how far down a design basis accident fault tree it has been possible for an incident to progress. From the evidence available here it appears that the policy of diversity of safety systems has been very successful.

During review of the draft of this paper, it was suggested to the author that 'the failures' which occurred during 'multiple failures incident' are not truly independent. The original causes of various latent failures may be independent, but the triggering of these failures, to produce serious consequences, is far from independent. This view is correct, and shows that the concept of 'independent failures' must be treated with care. A cable may be short circuited in two widely separated points by two different mechanisms (latent failures), but will only result in serious consequences, if electrical power is applied (triggering event). The fact remained that in reliability analyses, one must anticipate several independent latent failures.

It has also been pointed out that the definition of design error - a situation in which a failure leads to design modification - will automatically increase the number of recorded failures for an incident. This is in fact only true for those cases where material failure was the initiating incident, and where the design change was to avoid consequences of an incident of the same type i.e. where the failed component was replaced in its original form, but some additional safety measures were introduced. In any case, the surprising nature of the results gathered is not that incidents with many failures occur, but that the frequency of 3 fold failure, for example is not significantly different from the frequency for six fold or seven fold failure.

Analysis techniques have been developed to treat situations of the type observed in these studies (see e.g. D.S. Nielsen, 1973). It is hoped that some quantitative information about frequency and seriousness of multiple latent failures can be obtained, by application of the techniques to more detailed data, for which 'trivial failure' statistics exist, and for which the number of components at risk is known.

What can be done about design errors?

Design errors play a significant role in process plant failure. Design errors accounted for some 22% of reported safety related occurrences for light water reactors in 1971 (Classification of design errors, examples, and some statistics are given later).

It is not difficult to see why design errors occur. To dimension a single flow control valve requires some 20-30 design decisions. Some components especially those subject to high pressure, high temperature, or corrosive conditions, require many more. Systems design and investigations of component interactions require many more decisions. Routeing of electric and fluid control circuits to avoid common mode failures involves knowledge of a very large number of possible interactions. A modern process plant may contain in some cases hundreds of thousands of components each of which must be selected, individually dimensioned for its specific purpose, and its interactions with the rest of the system investigated.

Given that any human task is failure prone it may seem surprising that failures are not more frequent. Part of the answer is that designs are always based on earlier designs including relatively few new components. In this respect, accelerating development in techniques can give problems. A second part of the answer is that during construction, commissioning and testing, design failures are often found and corrected. This is no cause for overconfidence. Design errors are often sensitive to time and circumstance so that testing cannot find all the design failures in a system. The third reason that design errors are less frequent than might be expected, is that designs are checked by senior designers, by fitters, wiremen, and installation engineers who build the plant, and by the engineers, operators, and maintenance workers who eventually use the plant.

Just how bad the problem could be is seen by considering the case of computer programming. This task is almost pure design. Each page of program involves some hundred decisions. And each page of programs contains some two or three errors when first completed (by an experienced programmer). Testing takes two or three times as long as design, and even after extensive use, all large computer systems fail regularly. The largest systems fail due to design errors every few hours.

What can be done to reduce the number of design errors? One way of helping is to provide the designers with more information, in a more accessible form. Often in a design office, one lacks information on true component loadings, corrosion properties, and how a system is used in practice. Better feed back of information from plant users is almost always requested by designers, if they are asked.

Better use can generally be made of the experience of constructors and operators, as is shown by the success of 'suggestion box shemes' in many workshops. Given a chance, workmen responsible for installing and building equipment can almost always teach designers something about construction problems. They have also a better chance to learn of problems - intimate contact with a full size three dimensional plant, rather than the designers drawings.

Design checking is less reliable than the original design process. There is a psychological effect which leads people to accept information completely if it contains very few errors.

Making design checking more systematic helps a great deal in removing design errors. Such techniques as failure mode analysis, design check lists, and safety brainstorming are typical in this respect. Good working conditions, archive distribution, and systematic approval and countersigning of drawings also help. On-site cross checking between drawings and installed equipment and updating of drawings after on site equipment modifications, are steps which are often neglected. And proper safety checking after maintenance, repair, or modifications, is particularly difficult to ensure.

Computerised design represents an almost complete solution, in those areas where systematic design rules are possible. For example design of simple heat exchanger can be almost completely automated. If there are errors in design programs, they are generally gross errors and removed by simple manual cross checking of designs. A more subtle source of error is inappropriate design assumptions, or errors in design philosophy, which result in errors under special circumstances.

Computerised design is difficult. Selection of components, processes, and forms depends on very many influences, and a large amount of implicit information, which is very difficult to organise.

Human beings are extremely good at selection and satisfying multiple objectives.

Computerised checking of designs, on the other hand is in many cases easy. Once components have been selected, their properties and interrelations can be described, and their working evaluated.

Simulation is a prime technique for checking designs. Automatic techniques for checking designs are being developed, in the field of chemical processes (Powers) and control systems (Fussel) (Taylor) The techniques for computer aided piping design could be readily adapted to design checking. Techniques for checking for sneak paths in electrical circuits are available (Rankin). And the extension of control system techniques to complete system techniques, involve few changes in principle.

Extensions of techniques for checking controller designs (other examples mechanical design) could well be used for checking at least the written versions of operator instructions. Such a development would also be useful, in allowing more extensive interlock circuits to be designed, on the principle that any fault which can happen, will happen. (It should be remembered, though that not all failures can be prevented - interlocks cannot be designed to prevent failures arising from unknown phenomena, although diverse safety systems may do).

There is one major barrier to using computerised design checking. It takes time, effort, and money. Designers are often hard pressed, and their work critical to completion dates. They have no time to spend copying their drawings into computers. This is even more true for the most dangerous design task, design of a repair (most system failures occur after repair).

With systems which are really dangerous, or too complex to allow unrestricted modification, then rules for approval and inspection may be enforced. This can significantly reduce availability of process plant.

If computerised design checking techniques are to be used at all, the computer must become as convenient as drawing paper. It must be easier to use computer aided design than not to use it. This means larger display screens, with better resolution. It also means much better ergonomic design of computer aided design

Technique	Degree of use	Advantages	Disadvantages	Errors affected
1. Design follow-up at construction and commissioning	Usually only for major plant components	Better feedback to next plant design	Expensive in designer time	Communication
2. Design office information systems	Limited use e.g. SRS data base electronics components	A large proportion of lack of information errors limited	Expensive to keep updated	Communication
3. Systematic design procedure with drawing distribution lists, modification and 'incident' recording procedure	Widespread in process plant industry	Basic tool for ensuring adequate communication - when this breaks down errors occur	Large amounts of information are generated, not always in useful form for recipient	Communication
4. Independent design check	Atomic energy industry Aircraft industry Lloyds inspectors for process plant, ships	Spreads responsibility	Expensive checker cannot be involved in detail design, may miss errors	Oversight, calculation
5. Failure mode analysis	Aircraft, atomic, military, industries	Systematic	Expensive in engineer time	Oversight complex system
6. Cause consequence analysis	Aircraft, atomic military, industries	Systematic, more widely applicable than FMA	Expensive in engineer time	Oversight complex system
7. Design check lists	Widespread low level use	Simple	Difficult to make complete Difficult to apply effectively	Oversight
8. Computer aided design with built in design checks	Experimental-limited application areas	Cheap if computer aided design is used anyway. Thorough	Expensive to develop. Limited areas of application	Oversight calculation
9. Sneak path analysis	NASA	Thorough	Applies only to circuit faults	Complex system, oversight
10. Automatic failure mode Analysis, Cause consequence analysis	Experimental	Thorough	Requires development of large component data base. Expensive if applied independent of other design procedures	Complex system, oversight

Methods for reducing design error frequency

systems.

Computer aided design promises to make design more reliable, by making information more readily available (design catalogues on magnetic tape are already available), and by making it possible to check that the correct relationships between system components are fulfilled. This is a hopeful sign, at a time when industrial systems are becoming much more complex. There is also some hope that the study of principles of design, necessary for the computers benefit, can show how we can simplify our designs, rationalise their complexity, and better organise the ways we produce and understand them.

References

R.L. Scott and R.B. Gallaher	1971	'Safety Related Occurrences reported in 1971'. ORNL-NSIC-106.
D.S. Nielsen	1970	The cause consequence method as a basis for quantitative accident analysis. Report Risø-M-1374.
J.P. Rankin	1972	Sneak Circuit Analysis. Nuclear Safety Vol. 14, No 5, Sept.-Oct. 1973.
G. Powers	1974	Fault tree synthesis for chemical processes. A.I.Ch.E. Journal Vol. 20 No 2, March 1974.
J.B. Fussel	1973	A Formal methodology for fault tree construction. Nuclear Science and Engineering, Vol. 52, 421-432.
J.R. Taylor	1973	A semiautomatic method for failure mode analysis. Report Risø-M-1707.